Quantum Cloning Machines and the Applications

Heng Fan[1*], Yi-Nan Wang[2], Li Jing[2], Jie-Dong Yue[1], Han-Duo Shi [2], Yong-Liang Zhang [2], and Liang-Zhu Mu [2]

[1] *Beijing National Laboratory for Condensed Matter Physics, Institute of Physics, Chinese Academy of Sciences, Beijing 100190, China*
[2] *School of Physics, Peking University, Beijing 100871, China*

(Dated: January 25, 2013)

No-cloning theorem is fundamental for quantum mechanics and for quantum information science that states an unknown quantum state cannot be cloned perfectly. However, we can try to clone a quantum state approximately with the optimal fidelity, or instead, we can try to clone it perfectly with the largest probability. Thus various quantum cloning machines have been designed for different quantum information protocols. Specifically, quantum cloning machines can be designed to analyze the security of quantum key distribution protocols such as BB84 protocol, six-state protocol, B92 protocol and their generalizations. Some well-known quantum cloning machines include universal quantum cloning machine, phase-covariant cloning machine, the asymmetric quantum cloning machine and the probabilistic quantum cloning machine etc. In the past years, much progress has been made in studying quantum cloning machines and their applications and implementations, both theoretically and experimentally. In this review, we will give a complete description of those important developments about quantum cloning and some related topics. On the other hand, this review is self-consistent, and in particular, we try to present some detailed formulations so that further study can be taken based on those results. In addition, this review also contains some new results, for example, the study of quantum retrodiction protocol.

PACS numbers: 03.67.Ac, 03.65.Aa, 03.67.Dd, 03.65.Ta

Contents

* hfan@iphy.ac.cn

I. INTRODUCTION

In the past years, the study of quantum computation and quantum information has been attracting much attention from various research communities. Quantum information processing (QIP) is based on principles of quantum mechanics (Nielsen and Chuang, 2000). It promises algorithms which may surpass their classical counterparts. One of those algorithms is Shor algorithm (Shor, 1994) which can factorize large number exponentially faster than the existing classical algorithms do (Ekert and Jozsa, 1996). In this sense, the RSA public key cryptosystem (Rivest *et al.*, 1978) widely used in modern financial systems and networks might be attacked easily if a quantum computer exists, since the security of RSA system is based on assumption that it is extremely difficult to factorize a large number. On

the other hand, QIP provides an unconditional secure quantum cryptography based a principle of quantum mechanics, no-cloning theorem (Wootters and Zurek, 1982), which means that an unknown quantum state cannot be cloned perfectly.

For comparison, in classical information science, we use bit which is either "0" or "1" to carry the information, while for quantum information, a bit of quantum information which is named as "qubit" is encoded in a quantum state which may be a superposition of states $|0\rangle$ and $|1\rangle$. For example, a general qubit takes the form $\alpha|0\rangle + \beta|1\rangle$, where parameters α and β are complex numbers according to quantum mechanics and are normalized as $|\alpha|^2 + |\beta|^2 = 1$. So a qubit can collapse to either $|0\rangle$ or $|1\rangle$ with some probability if a measurement is performed. The classical information can be copied perfectly. We know that we can copy a file in a computer without any principal restriction. On the contrary, QIP is based on principles of quantum mechanics, which is linear and thus an arbitrary quantum state cannot be cloned perfectly since of the no-cloning theorem. We use generally terminology "clone" instead of "copy" for reason of no-cloning theorem in (Wootters and Zurek, 1982). No-cloning, however, is not the end of the story.

It is prohibited to have a perfect quantum clone. It is still possible that we can copy a quantum state approximately or probabilistically. There are various quantum protocols for QIP which may use tool of quantum cloning for different goals. Thus various quantum cloning machines have been created both theoretically and experimentally. The study of quantum cloning is of fundamental interest in QIP. Additionally, the quantum cloning machines can also be applied directly in various quantum key distribution (QKD) protocols. The first quantum key distribution protocol proposed by Bennett and Brassard in 1984 (BB84) uses four different qubits, BB84 states (Bennett and Brassard, 1984), to encode classical information in transmission. Correspondingly, the phase-covariant quantum clone machine, which can copy optimally all qubits located in the equator of the Bloch sphere, is proved to be optimal for cloning of states similar as BB84 states. The BB84 protocol can be extended to six-state protocol, the corresponding cloning machine is the universal quantum cloning machine which can copy optimally arbitrary qubits. Similarly the probabilistic quantum cloning machine is for B92 QKD protocol (Bennett, 1992). Quantum cloning is also related with some fundamentals in quantum information science, for example, the no-cloning theorem is closely related with no-signaling theorem which means that superluminal communication is forbidden. We can also use quantum cloning machines for estimating a quantum state or phase information of a quantum state. So the study of quantum cloning is of interest for reasons of both fundamental and practical applications.

The previous well-accepted reviews of quantum cloning can be found in (Scarani *et al.*, 2005), and also in (Cerf and Fiurášek, 2006). Quantum cloning, as other topics of quantum information, developed very fast in the past years. An up-to-date review is necessary. In the present review, we plan to give a full description of results about quantum cloning and some closely related topics. This review is self-consistent and some fundamental knowledge is also introduced. In particular, a main characteristic of this review is that it contains a large number of detailed formulations for the main review topics. It is thus easy to follow those calculations for further study about those quantum cloning topics. We also incorporate some unpublished new results into this review so that it is worth for experts of quantum cloning to have a look of those new ideas.

The review is organized as follows: In the next part of this section, we will present in detail some fundamental concepts of quantum computation and quantum information including the form of qubit represented in Bloch sphere, the definition of entangled state, some principles of quantum mechanics used in the review. Then we will present in detail the developments of quantum cloning. Here let us introduce briefly some results contained in this review. In Section II, we will review several proofs of no-cloning theorem from different points of view, including a simple presentation, no-cloning for mixed states, the relationship between no-cloning and no-signaling theorems for quantum states, no-cloning from information theoretical viewpoints. In Section III, we will review the universal quantum cloning machine. We will present the universal quantum cloning machine for qubit and qudit including both symmetric and asymmetric cases. We then will present a unified quantum cloning machine which can be easily reduced to several universal cloning machines. We will also show some schemes for cloning of mixed states. We will show that the universal quantum cloning machine, by definition, can copy arbitrary input state, is necessary for a six-state input which are used in QKD. Further, the universal cloning machine is necessary for a four-state input which is the minimal input set. In Section V, the phase-covariant quantum cloning machines will be presented. One important application of this cloning machine is to study the well-known BB84 quantum cryptography. The phase-covariant quantum cloning machines include the cases of qubit and of higher dimension. In particular, a unified phase-covariant quantum cloning machine will be presented which can be adjusted for an arbitrary subset of the mutually unbiased bases. We can also show that the minimal input for phase-covariant quantum cloning is a set of three states with equal phase distances in the equator of Bloch sphere. The phase-covariant quantum cloning is actually state-dependent, we thus will present some other cases of state-dependent quantum cloning.

In section IX, the security analysis of QKD based on mean king retrodiction protocol will be presented. The main results in this section are new.

In section X, we present some detailed results of sequential quantum cloning which are not published before.

In order to have a full view of all developments in quantum cloning and some closely related topics, we try to review

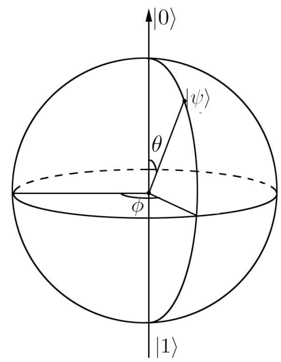


FIG. 1 (color online). A qubit in Bloch sphere, $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle$, it contains amplitude parameter θ and phase parameter ϕ.

some references briefly in one to two sentences. Those parts are generally named as 'other developments and related topics'. Our aim is to cover as much as possible these developments in quantum cloning, but we understand that some important references might still be missed in this review.

A. Quantum information, qubit and quantum entanglement

We have a quantum system constituted by two states $|0\rangle$ and $|1\rangle$. They are orthogonal,

$$\langle 0|1\rangle = 0. \tag{1}$$

Those two states can be energy levels of an atom, photon polarizations, electron spins, Bose-Einstein condensate with two intrinsic freedoms or any physical material with quantum properties. In this review, we also use some other standard notations $|0\rangle = |\uparrow\rangle, |1\rangle = |\downarrow\rangle$ and exchange them without mentioning. Simply, those two states can be represented as two vectors in linear algebra,

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2}$$

Corresponding to bit in classical information science, a qubit in quantum information science is a superposition of two orthogonal states,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{3}$$

where a normalization equation should be satisfied,

$$|\alpha|^2 + |\beta|^2 = 1. \tag{4}$$

Here both α and β are complex parameters which include amplitude and phase information, $\alpha = |\alpha|e^{i\phi_\alpha}$ and $\beta = |\beta|e^{i\phi_\beta}$. So a qubit $|\psi\rangle$ is defined on a two-dimensional Hilbert space $\mathbb{C}^2$. In quantum mechanics, a whole phase cannot be detected and thus can be omitted, only the relative phase of α and β is important which is $\phi = \phi_\alpha - \phi_\beta$. Now we can find that a qubit can be represented in another form,

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle, \tag{5}$$

where $\theta \in [0, \pi], \phi \in [0, 2\pi\}$. It corresponds to a point in the Bloch sphere, see FIG. 1.

The two qubits in separable form can be written as,

$$\begin{aligned} |\psi\rangle|\phi\rangle &= (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle) \\ &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \alpha\delta|11\rangle. \end{aligned} \tag{6}$$

If those two qubits are identical, one can find,

$$\begin{aligned} |\psi\rangle^{\otimes 2} &\equiv (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha^2|00\rangle + \sqrt{2}\alpha\beta\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) + \beta^2|11\rangle. \end{aligned} \tag{7}$$

For convenience, we write the second term as a normalized symmetric state $\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)$ which will be used later.

For two-qubit state, besides those separable state, we also have the entangled state, for example,

$$|\Phi^+\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle). \tag{8}$$

This is state cannot be written as a product form like $|\psi\rangle|\phi\rangle$, so it is "entangled". It is actually a maximally entangled state. In quantum information science, quantum entanglement is the valuable resource which can be widely used in various tasks and protocols. Complementary to entangled state $|\Phi^+\rangle$, we have other three orthogonal and maximally entangled state which constitute a complete basis for $\mathbb{C}^2\otimes\mathbb{C}^2$. Those four states are Bell states, here we list them all as follows,

$$\begin{aligned}
|\Phi^+\rangle &\equiv \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle), && (9)\\
|\Phi^-\rangle &\equiv \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle), && (10)\\
|\Psi^+\rangle &\equiv \frac{1}{\sqrt{2}}(|01\rangle+|10\rangle), && (11)\\
|\Psi^-\rangle &\equiv \frac{1}{\sqrt{2}}(|01\rangle-|10\rangle). && (12)
\end{aligned}$$

Those four Bell states can be transformed to each other by local unitary transformations.

Consider three Pauli matrices defined as,

$$\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad \sigma_y=\begin{pmatrix}0&-i\\i&0\end{pmatrix},\quad \sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}. \tag{13}$$

Since $\sigma_y=i\sigma_x\sigma_z$, if the imaginary unit, "i", is the whole phase, we sometimes use $\sigma_x\sigma_z$ instead of σ_y. Bear in mind that we have $|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$, and $\langle 0|=(1,0)$, so in linear algebra, we have the representation,

$$|0\rangle\langle 0|=\begin{pmatrix}1\\0\end{pmatrix}(1,0)=\begin{pmatrix}1&0\\0&0\end{pmatrix}. \tag{14}$$

Now three Pauli matrices have an operator representation,

$$\begin{aligned}
\sigma_x &= |0\rangle\langle 1|+|1\rangle\langle 0|, && (15)\\
\sigma_y &= -i|0\rangle\langle 1|+i|1\rangle\langle 0|, && (16)\\
\sigma_z &= |0\rangle\langle 0|-|1\rangle\langle 1|. && (17)
\end{aligned}$$

In this review, we will not distinguish the matrix representation and the operator representation. Acting Pauli matrices σ_x and σ_z on a qubit, we find,

$$\begin{aligned}
\sigma_x|0\rangle=|1\rangle,\quad \sigma_x|1\rangle=|0\rangle, && (18)\\
\sigma_z|0\rangle=|0\rangle,\quad \sigma_z|1\rangle=-|1\rangle, && (19)
\end{aligned}$$

which are the bit flip action and phase flip action, respectively, while σ_y will cause both bit flip and phase flip for a qubit. In this review, for convenience, we sometimes use notations $X\equiv\sigma_x, Z\equiv\sigma_z$ to represent the corresponding Pauli matrices. Also, those Pauli matrices can also be defined in higher dimensional system, while the same notations might be used if no confusion is caused.

For four Bell states, their relationship by local transformations can be as follows,

$$\begin{aligned}
|\Phi^-\rangle &= (I\otimes\sigma_z)|\Phi^+\rangle, && (20)\\
|\Psi^+\rangle &= (I\otimes\sigma_x)|\Phi^+\rangle, && (21)\\
|\Psi^-\rangle &= (I\otimes\sigma_x\sigma_z)|\Phi^+\rangle, && (22)
\end{aligned}$$

where I is the identity in $\mathbb{C}^2$, the Pauli matrices are acting on the second qubit.

Here we have already used the tensor product. Consider two operators, $O_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$, $O_2 = \begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix}$, the tensor product $O_1 \otimes O_2$ is defined and calculated as follows,

$$\begin{aligned} O_1 \otimes O_2 &= \begin{pmatrix} A_1 O_2 & B_1 O_2 \\ C_1 O_2 & D_1 O_2 \end{pmatrix} \\ &= \begin{pmatrix} A_1A_2 & A_1B_2 & B_1A_2 & B_1B_2 \\ A_1C_2 & A_1D_2 & B_1C_2 & B_1D_2 \\ C_1A_2 & C_1B_2 & D_1A_2 & D_1B_2 \\ C_1C_2 & C_1D_2 & D_1C_2 & D_1D_2 \end{pmatrix}. \end{aligned} \tag{23}$$

When we apply a tensor product of, $O_1 \otimes O_2$, on a two-qubit quantum state, operator O_1 is acting on the first qubit, operator O_2 is acting on the second qubit.

We have already extended one qubit to two-qubit state. Similarly, multipartite qubit state can be obtained. Also we may try to extend qubit from two-dimension to higher-dimensional system, generally named as "qutrit" for dimension three and "qudit" for dimension d in more general case, the Hilbert space is extended from $\mathbb{C}^2$ to $\mathbb{C}^d$. For example, we sometimes have "qutrit" when we consider a quantum state in three dimensional system. For more general case, a qudit is also a superposed state,

$$|\psi\rangle = \sum_{j=0}^{d-1} x_j |j\rangle, \tag{24}$$

where $x_j, j = 0, 1, ..., d-1$, are normalized complex parameters. Quantum entanglement can also be in higher dimensional, multipartite systems.

A qubit $|\psi\rangle$ can be represented by its density matrix,

$$\begin{aligned} |\psi\rangle\langle\psi| &= (\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle 0| + \beta^*\langle 1|) \\ &= \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix}. \end{aligned} \tag{25}$$

However, a general qubit may be not only the superposed state, which is actually the pure state, but also a mixed state which is in a probabilistic form. It can only be represented by a density operator ρ,

$$\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|, \tag{26}$$

where p_j is the probabilistic distribution with $\sum p_j = 1$.

A density matrix is positive semi-definite, and its trace equals to 1,

$$\rho \geq 0, \quad \mathrm{Tr}\rho = 1. \tag{27}$$

The density matrices of a pure state and a mixed state can be easily distinguished by the following conditions,

$$\mathrm{Tr}\rho^2 = 1, \quad \text{pure state}; \tag{28}$$

$$\mathrm{Tr}\rho^2 < 1, \quad \text{mixed state}. \tag{29}$$

For multipartite state, one part of the state is the reduced density matrix obtained by tracing out other parts. For example, for two-qubit maximally entangled state $|\Phi^+_{AB}\rangle$ constituted by A and B parts, each qubit is a mixed state,

$$\rho_A = \mathrm{Tr}_B |\Phi^+_{AB}\rangle\langle\Phi^+_{AB}| = \frac{1}{2} I. \tag{30}$$

This case is actually a completely mixed state. The density operator can be written as any pure state and its orthogonal state with equal probability,

$$\rho_A = \frac{1}{2} I = \frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{2}|\psi^\perp\rangle\langle\psi^\perp|, \tag{31}$$

where if $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, its orthogonal state can take the form,

$$|\psi^\perp\rangle = \beta^*|0\rangle - \alpha^*|1\rangle, \tag{32}$$

where $*$ means the complex conjugation.

B. Quantum gates

In QIP, all operations should satisfy the laws of quantum mechanics such as the generally used unitary transformation and quantum measurement. Similar as in classical computation, all quantum computation can be effectively implemented by several fundamental gates. The single qubit rotation gate and controlled-NOT (CNOT) gate constitute a complete set of fundamental gates for universal quantum computation (Barenco *et al.*, 1995). The single qubit rotation gate is just a unitary transformation on a qubit, $\hat{R}(\vartheta)$, defined as

$$\begin{aligned} \hat{R}(\vartheta)|0\rangle &= \cos\vartheta|0\rangle + e^{i\phi}\sin\vartheta|1\rangle, \\ \hat{R}(\vartheta)|1\rangle &= -e^{-i\phi}\sin\vartheta|0\rangle + \cos\vartheta|1\rangle, \end{aligned} \tag{33}$$

where the phase parameter ϕ should also be controllable. The CNOT gate is defined as a unitary transformation on two-qubit system, one qubit is the controlled qubit and another qubit is the target qubit. For a CNOT gate, when the controlled qubit is $|0\rangle$, the target qubit does not change; when the controlled qubit is $|1\rangle$, the target qubit should be flipped. Explicitly it is defined as,

$$\begin{aligned} &CNOT : |0\rangle|0\rangle \rightarrow |0\rangle|0\rangle; \\ &CNOT : |0\rangle|1\rangle \rightarrow |0\rangle|1\rangle; \\ &CNOT : |1\rangle|0\rangle \rightarrow |1\rangle|1\rangle; \\ &CNOT : |1\rangle|1\rangle \rightarrow |1\rangle|0\rangle, \end{aligned} \tag{34}$$

where the first qubit is the controlled qubit and the second qubit is the target qubit. By matrix representation, CNOT gate takes the form,

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{35}$$

Depending on physical systems, we can use different universal sets of quantum gates to realize the universal quantum computation.

II. NO-CLONING THEOREM

A. A simple proof of no-cloning theorem

For classical information, the possibility of cloning it is an essential feature. In classical systems, cloning, in other words, copying seems no problem. Information stored in computers can be easily made several copies as backup; the accurate semiconservative replication of DNA steadily passes gene information between generations. But for quantum systems, this is not the case. As proved by Wootters and Zurek (Wootters and Zurek, 1982), deterministic cloning of pure states is not possible. After this seminal work, much interest has been shown in extending and generalizing the original no-cloning theorem(Barnum *et al.*, 1996; Luo, 2010b; Luo *et al.*, 2009; Luo and Sun, 2010; Piani *et al.*, 2008), which gives us new insight to boundaries of the classical and quantum. On the other hand, no-signaling, guaranteed by Einstein's theory of relativity, is also delicately preserved by no-cloning. This chapter will focus on these topics, hoping to give a thorough description of the no-cloning theorem.

As it is known, a single measurement on a quantum system will only reveal minor information about it, but as a result of which, the quantum system will collapse to an eigenstate of the measurement operator and all the other information about the original state becomes lost. Suppose there exists a cloning machine with a quantum operation U, which duplicates an arbitrary pure state

$$U(|\varphi\rangle \otimes |R\rangle \otimes |M\rangle) = |\varphi\rangle \otimes |\varphi\rangle \otimes |M(\varphi)\rangle \tag{36}$$

here $|\varphi\rangle$ denotes an arbitrary pure state, $|R\rangle$ an initial blank state of the cloning machine, $|M\rangle$ the initial state of the auxiliary state(ancilla), and $M(\varphi)\rangle$ is the ancillary state after operation which depends on $|\varphi\rangle$. With such machine, one can get any number of copies of the original quantum state, and then complete information of it can be determined. However, is it possible to really build such a machine? No-cloning theorem says no.

THEOREM : No quantum operation exist which can perfectly and deterministically duplicate a pure state.

The proof comes in 2 ways.

(1). Using the linearity of quantum mechanics. This proof is first proposed by Wootters and Zurek (Wootters and Zurek, 1982). Suppose there exists a perfect cloning machine that can copy an arbitrary quantum state, that is, for any state $|\varphi\rangle$

$$|\varphi\rangle|\Sigma\rangle|M\rangle \rightarrow |\varphi\rangle|\varphi\rangle|M(\varphi)\rangle$$

where $|\Sigma\rangle$ is a blank state, and $|M\rangle$ is the state of auxiliary system(ancilla). Thus for state $|0\rangle$ and $|1\rangle$, we have

$$|0\rangle|\Sigma\rangle|M\rangle \rightarrow |0\rangle|0\rangle|M(0)\rangle,$$

$$|1\rangle|\Sigma\rangle|M\rangle \rightarrow .|1\rangle|1\rangle|M(1)\rangle$$

In this way, for the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$(\alpha|0\rangle + \beta|1\rangle)|\Sigma\rangle|M\rangle \rightarrow \alpha|00\rangle|M(0)\rangle + \beta|11\rangle|M(1)\rangle$$

On the other hand, $|\psi\rangle$ itself is a pure state, so

$$|\psi\rangle|\Sigma\rangle|M\rangle \rightarrow (\alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle)|M(\psi)\rangle.$$

Obviously, the right hand sides of the two equations cannot be equal, as a result, the premise is false that such a perfect cloning machine exists, which concludes the proof.

(2). Using the properties of unitary operation. This proof can be found in Sec. 9-4 of Peres's textbook(Peres, 1995). Consider the process of cloning machine as a unitary operator U, then for any two state $|\varphi\rangle$ and $|\psi\rangle$, since under unitary operation the inner product is preserved, we have

$$\langle\psi|\varphi\rangle = \langle\psi|U^\dagger U\varphi\rangle = \langle\psi|\langle\psi|\varphi\rangle|\varphi\rangle = \langle\psi|\varphi\rangle^2$$

So $\langle\psi|\varphi\rangle$ is either 0 or 1. If the value is 0, it means the two states being copied should be orthogonal, while if 1, the two states are the same.

B. No-broadcasting theorem

Following the no cloning theorem for pure states, the impossibility of cloning a mixed state is later proved by Barnum *et al.* (Barnum *et al.*, 1996). In fact, rather than cloning, broadcasting, whose meaning will be presented later in this section, is prohibited by quantum mechanics. Correlations, as a fundamental theme of science, is also studied in quantum systems. An elegant no local broadcasting theorem for correlations in a multipartite state is proposed by Piani *et al.* (Piani *et al.*, 2008). With these two no-broadcasting theorems, it is natural to ask what is the relationship between them. Recently Luo *et al.* have established the no-unilocal broadcasting theorem for quantum correlations, which proves to be the bridge between Barnum's and Piani's theorems and with it we are able to build the equivalence between them. The three theorems together would give us a unified picture of no-broadcasting in quantum systems.

We shall first elaborate on the original no-broadcasting theorem for non-commuting states proposed by Barnum *et al.*(Barnum *et al.*, 1996). Suppose there are two parts A and B of a composite quantum system AB, A is prepared in one of the states $\{\sigma_i\}$, while B is prepared in the blank state τ. If there exists a quantum operation $\mathcal{E}$ which can be performed on system AB, that is, $\sigma_k \otimes \tau \to \mathcal{E}(\sigma_k \otimes \tau) = \rho_k^{out}$ and the output state satisfies

$$\mathrm{Tr}_a \rho_k^{out} = \sigma_k \quad \text{and } \mathrm{Tr}_b \rho_k^{out} = \sigma_k,\ \forall k,$$

we say $\mathcal{E}$ broadcasts the set of states $\{\sigma_i\}$, notice that we have not considered the ancilla, which will not affect generality since it will be traced out in computation, so we won't introduce the ancilla in the following text as well. Here comes Barnum's theorem(Barnum *et al.*, 1996)

Theorem 1. A set of states $\{\sigma_i\}$ is broadcastable if and only if the states commute with each other.

Several kinds of proof for Theorem 1 have been found (Barnum *et al.*, 2007, 1996; Kalev and Hen, 2008; Lindblad, 1999), one of them is provided as follows using the property of relative entropy (Kalev and Hen, 2008). We shall only prove Theorem 1 in the case that the set $\{\sigma_i\}$ only have two states σ_1 and σ_2, from which more complex cases can be easily extended to.

Proof for Theorem 1

1) "if" part: since σ_1 and σ_2 commute, they can be expressed in the same orthonormal basis $\{|i\rangle\}$:

$$\sigma_k = \sum_i \lambda_{k,i} |i\rangle\langle i|,\ k = 1, 2.$$

Because $\{|i\rangle\}$ is an orthonormal set, it can be cloned by an operator $\mathcal{E}$, so we get

$$\rho_k^{out} = \mathcal{E}(\sigma_k \otimes \tau) = \sum_i \lambda_{k,i} |ii\rangle\langle ii|,\ k = 1, 2,$$

thus

$$\mathrm{Tr}_a \rho_k^{out} = \sigma_k, \quad \mathrm{Tr}_b \rho_k^{out} = \sigma_k,\ k = 1, 2.$$

So we see σ_1 and σ_2 are broadcasted by $\mathcal{E}$.

2) "only if" part: first we shall introduce the concept of relative entropy. The relative entropy S of ρ_1 with respect to ρ_2 is defined as(Umegaki and Ködai, 1962)

$$S(\rho_1|\rho_2) = \mathrm{Tr}[\rho_1(\ln \rho_1 - \ln \rho_2)].$$

When $ker(\rho_1)^{\perp} \bigcap ker(\rho_2) = 0$, S is well-defined, otherwise S leads to ∞ (Wehrl, 1978). We first consider the case $ker(\rho_2) \subseteq ker(\rho_1)$, then $S < \infty$. Denote $S_1^i n = \sigma_1 \otimes \tau$ and $S_2^i n = \sigma_2 \otimes \tau$, we get

$$\begin{aligned} S(\rho_1^{in}|\rho_2^{in}) &= \mathrm{Tr}[\sigma_1 \otimes \tau(\log \sigma_1 \oplus \log \tau - \log \sigma_2 \oplus \log \tau] \\ &= \mathrm{Tr}_a[\sigma_1(\log \sigma_1 - \log \sigma_2)]\mathrm{Tr}_b \tau \\ &= \mathrm{Tr}_a[\sigma_1(\log \sigma_1 - \log \sigma_2)] \\ &= S(\sigma_1|\sigma_2). \end{aligned}$$

Because for any quantum operation $\mathcal{E}$, $S(\mathcal{E}(\rho_1)|\mathcal{E}(\rho_2)) = S(\rho_1|\rho_2)$, we have

$$S(\sigma_1|\sigma_2) = S(\rho_1^{in}|\rho_2^{in}) = S(\rho_1^{out}|\rho_2^{out}).$$

Next we invoke the monotonocity of relative entropy(Lindblad, 1975)

$$S(\rho_1^{ab}|\rho_2^{ab}) \geq S(\rho_1^b|\rho_2^b),$$

where ρ_1^b denotes the reduced density matrix of the composite system ρ_1^{ab}, and the equality holds if and only if the following condition is satisfied:

$$\log\rho_1^{ab} - \log\rho_2^{ab} = I^a \otimes (\log\rho_1^b - \log\rho_2^b).$$

So we have

$$S(\rho_1^{out}|\rho_2^{out}) \geq S(\rho_1^{k,out}|\rho_2^{k,out}), \tag{37}$$

for k=a,b where $\rho_i^{k,out}$ denotes $Tr_{a(b)}\rho_i^{out}$. The equality holds if and only if

$$\begin{aligned}\log\rho_1^{out} - \log\rho_2^{out} &= (\log\rho_1^{a,out} - \log\rho_2^{a,out}) \otimes I^b \\ &= I^a \otimes (\log\rho_1^{b,out} - \log\rho_2^{b,out}).\end{aligned}$$

Under the broadcasting condition, we get

$$\begin{aligned}\log\rho_1^{out} - \log\rho_2^{out} &= (\log\sigma_1 - \log\sigma_2) \otimes I^b \\ &= I^a \otimes (\log\sigma_1 - \log\sigma_2).\end{aligned}$$

But the above equation holds only when σ_1 and σ_2 are diagonal or they can be diagonalized in the same basis, which means they commute.

For the case $S(\sigma_1|\sigma_2) = \infty$, we consider a mixed state $\sigma_{mix} = \lambda\sigma_1 + (1-\lambda)\sigma_2$, where $0 < \lambda < 1$. If σ_1 and σ_2 can be broadcast, then so can be σ_1 and σ_{mix}, due to linearity of the operation. But $ker(\sigma_{mix}) \subseteq ker(\sigma_1)$, thus σ_1 and σ_{mix} commute, so σ_1 and σ_2 commute. Now we have finished the proof of Theorem 1.

C. No-broadcasting for correlations

The quantum entanglement differs quantum world from classical world. Recently, it is also realized that quantum correlation, which may be beyond the quantum entanglement, is also important for QIP. Here we can first make a classification of states by correlation(Piani *et al.*, 2008). For a bipartite state ρ^{ab} shared by two parties A and B, it is called separable if it can be decomposed as

$$\rho^{ab} = \Sigma_j p_j \rho_j^a \otimes \rho_j^b,$$

where $\{p_j\}$ denotes a probability distribution, $\{\rho_j^a\}$ and $\{\rho_j^b\}$ denote states of party a and b. Otherwise, the ρ^{ab} is called entangled.

If ρ^{ab} can be further decomposed as

$$\rho^{ab} = \Sigma_i p_i |i\rangle\langle i| \otimes \rho_i^b,$$

with $\{p_i\}$ denoting a probability distribution, $\{|i\rangle\}$ a orthonormal set of party a and $\{\rho_i^b\}$ states of party b, we say it is classical-quantum.

If ρ_i^b can also be represented in an orthonormal set $\{|j\rangle\}$, which makes

$$\rho^{ab} = \Sigma_i p_{ij} |i\rangle\langle i| \otimes |j\rangle\langle j|,$$

where $\{p_{ij}\}$ represents a probability distribution for two variables, we say it is classical(or classical-classical).

As we know the correlation in ρ^{ab} can be quantified by mutual information

$$I(\rho^{ab}) = S(\rho^a) + S(\rho^b) - S(\rho^{ab}),$$

where S denotes the von Neumann entropy, that is, $S(\rho) = -\mathrm{Tr}(\rho\ln\rho)$.

We say the correlation in ρ^{ab} is locally broadcast if there exists two quantum operations $\mathcal{E}^a : \mathcal{S}(H^a) \to \mathcal{S}(H^{a_1} \otimes H^{a_2})$ and $\mathcal{E}^b : \mathcal{S}(H^b) \to \mathcal{S}(H^{b_1} \otimes H^{b_2})$, here $\mathcal{S}(H)$ denotes the set of quantum states on Hilbert space H, such that

$\rho^{ab} \to (\mathcal{E}^a \otimes \mathcal{E}^b)\rho^{ab} = \rho^{a_1a_2b_1b_2}$, and the amount of correlations in the two reduced states $\rho^{a_1b_1} = \mathrm{Tr}_{a_2b_2}\rho^{a_1a_2b_1b_2}$ and $\rho^{a_2b_2} = \mathrm{Tr}_{a_1b_1}\rho^{a_1a_2b_1b_2}$ is identical to which of ρ^{ab}, that is

$$I(\rho^{a_1b_1}) = I(\rho^{a_2b_2}) = I(\rho^{ab}).$$

While suppose there is a quantum operation $\mathcal{E}^a$ performed on party a, and we get $(\mathcal{E}^a \otimes I^b)\rho^{ab} = \rho^{a_1a_2b}$, we say the correlation in ρ^{ab} is locally broadcast by party a if

$$I(\rho^{a_1b}) = I(\rho^{a_2b}) = I(\rho^{ab}),$$

where $\rho^{a_1b} = \mathrm{Tr}_{a_2}\rho^{a_1a_2b}$ and $\rho^{a_2b} = \mathrm{Tr}_{a_1}\rho^{a_1a_2b}$.

With the above definition, we can then state no-broadcasting theorems for correlation proposed by Piani *et al.* and Luo *et al.*

Theorem 2: The correlation in a bipartite state can be locally broadcast if and only if the state is classical.

Theorem 3: The correlation in the bipartite state ρ^{ab} can be locally broadcast by party a if and only if ρ^{ab} is classical-quantum.

D. A unified no-cloning theorem from information theoretical point of view

Now we shall build equivalence among the theorems according to the method proposed by Luo *et al.*(Luo, 2010b; Luo and Sun, 2010), that is,

Theorem 1 $\Leftrightarrow$ Theorem 2 $\Leftrightarrow$ Theorem 3.

First we shall establish a lemma.

Lemma 1: Any bipartite state can be decomposed as

$$\rho^{ab} = \sum_k X_k^a \otimes X_k^b,$$

where each X_k^a is non-negative and $\{X_k^b\}$ forms a linearly independent set.

Proof: Let $\{Y_j^a\}$ be a linearly independent set for party a, $\{Z_k^b\}$ a linearly independent set for party b. Then any bipartite state ρ^{ab} can be decomposed in the basis $\{Y_j^a \otimes Z_k^b\}$, that is

$$\rho^{ab} = \sum_{jk} \lambda_{jk} Y_j^a \otimes Z_k^b.$$

Obviously we can let $Z_k^a = \sum_j \lambda_{jk} Y_j^a$ and obtain

$$\rho^{ab} = \sum_k Z_k^a \otimes Z_k^b. \tag{38}$$

Notice that Z_k^a need not to be non-negative, so we have not arrived at Lemma 1 yet. Starting from (38), we take a fixed $|y\rangle \in H^b$ such that

$$c_1 = \langle y|Z_1^b|y\rangle \neq 0,$$

let $c_k = \langle y|Z_k^b|y\rangle$, we can write ρ^{ab} as

$$\begin{aligned}
\rho^{ab} &= \sum_k Z_k^a \otimes Z_k^b \\
&= \sum_k Z_k^a \otimes Z_k^b + \sum_{k\neq 1} \frac{c_k}{c_1} Z_k^a \otimes Z_1^b - \sum_{k\neq 1} Z_k^a \otimes \frac{c_k}{c_1} Z_1^b \\
&= (Z_1^a + \sum_{k\neq 1} \frac{c_k}{c_1} Z_k^a) \otimes Z_1^b + \sum_{k\neq 1} Z_k^a \otimes (Z_k^b - \frac{c_k}{c_1} Z_1^b) \\
&= X_1^a \otimes Z_1^b + \sum_{k\neq 1} Z_k^a \otimes \widetilde{Z_k^b},
\end{aligned}$$

where $X_1^a = Z_1^a + \sum_{k\neq 1} \frac{c_k}{c_1} Z_k^a$ and $\widetilde{Z_k^b} = Z_k^b - \frac{c_k}{c_1} Z_1^b$

Because for any k,

$$\langle y|\widetilde{Z_k^b}|y\rangle = \langle y|(Z_k^b - \frac{c_k}{c_1}Z_1^b)|y\rangle = c_k - \frac{c_k}{c_1}c_1 = 0,$$

together with the non-negative property of density operator ρ^{ab},we have for any $|x\rangle \in H^a$

$$\begin{aligned}\langle x\otimes y|\rho^{ab}|x\otimes y\rangle &= \langle x|X_1^a|x\rangle\langle y|Z_1^b|y\rangle + \sum_{k\neq 1}\langle x|Z_k^a|x\rangle\langle y|\widetilde{Z_k^b}|y\rangle \\ &= c_1\langle x|X_1^a|x\rangle \\ &\geq 0.\end{aligned}$$

Since $c_1 \neq 0$, we see X_1^a or $-X_1^a$ is non-negative depending on the sign of c_1. Without loss of generality, we can always assume X_1^a to be non-negative, because the negative sign can be absorbed by Z_1^b. Further we see the set $\{Z_1^b, \widetilde{Z_k^b}\}$ still forms a linearly independent set.

Now all the $Z_i^a(i \leq 2)$ and Z_1^b remain unchanged, and replace Z_1^a with X_1^a, $Z_j^b(j \geq 2)$ with $\widetilde{Z_j^b}$, we can find a $|\widetilde{y}\rangle \in H^b$ such that $\langle\widetilde{y}|\widetilde{Z_2^b}|\widetilde{y}\rangle \neq 0$, continue the above process, we would have got X_2^a which is non-negative. Finally we can replace all the Z_i^a's with X_i^a's and thus the proof is completed.

Next we prove Theorem 1 $\Rightarrow$ Theorem 3.

Proof: ("if" part) Since ρ^{ab} is a classical-quantum state, it can be rewritten as

$$\rho^{ab} = \sum_i p_i|i\rangle\langle i| \otimes \rho_i^b,$$

where $\{|i\rangle\}$ is a linearly independent set, we can further assume it to be an orthonormal base, otherwise we may need to append some zero p_i. For any state $\sigma \in S(H^a)$, construct a quantum map $\mathcal{E}^a : S(H^a) \to S(H^{a_1}) \otimes S(H^{a_2})$ such that

$$\mathcal{E}^a(\sigma) = \sum_i E_i\sigma E_i^\dagger \tag{39}$$

where $E_i = |ii\rangle\langle i|$. Perform $\mathcal{E}$ on party a, then we have locally broadcast ρ^a, and of course the correlation in ρ^{ab} is locally broadcast by party a as well.

("only if" part) Suppose the correlation in ρ^{ab} is locally broadcast by party a through the operator $\mathcal{E}^a : \mathcal{S}(H^a) \to \mathcal{S}(H^{a_1} \otimes H^{a_2})$, then

$$\rho^{a_1a_2b} = \mathcal{E}^a \otimes \mathcal{I}^b(\rho^{ab}),$$

where $\mathcal{I}^b$ is the identity operator on H^b. We have

$$I(\rho^{a_1b}) = I(\rho^{a_2b}) = I(\rho^{ab}).$$

Denote the operator $\mathcal{T}_{a_2}^{a_1a_2} : \mathcal{S}(H^{a_1} \otimes H^{a_2}) \to \mathcal{S}(H^{a_1})$ as the partial tracing operator by tracing out a_2, thus

$$\rho^{a_1b} = (\mathcal{T}_{a_2}^{a_1a_2} \otimes \mathcal{I}^b)(\rho^{a_1a_2b}) = \mathcal{T}_{a_2}^{a_1a_2}\mathcal{E}^a \otimes \mathcal{I}^b(\rho^{ab}).$$

According to the condition

$$I(\rho^{a_1b}) = I(\rho^{ab}),$$

and notice that $I(\rho^{ab}) = S(\rho^{ab}|\rho^a \otimes \rho^b)$, where S is the relative entropy, ρ^a and ρ^b stand for reduced states, we have

$$S(\mathcal{T}_{a_2}^{a_1a_2}\mathcal{E}^a \otimes \mathcal{I}^b(\rho^{ab})|\mathcal{T}_{a_2}^{a_1a_2}\mathcal{E}^a \otimes \mathcal{I}^b(\rho^a \otimes \rho^b)) = S(\rho^{ab}|\rho^a \otimes \rho^b). \tag{40}$$

Now we shall introduce a theorem stating that(Lindblad, 1975)

$$S(\rho|\sigma) \geq S(\mathcal{E}(\rho)|\mathcal{E}(\sigma)) \tag{41}$$

for any quantum state ρ and σ, and any quantum map $\mathcal{E} : \mathcal{S}(H) \to \mathcal{S}(K)$.

The equality holds if and only if there exists an operator $\mathcal{F} : \mathcal{S}(K) \to \mathcal{S}(H)$ such that

$$\mathcal{F}\mathcal{E}(\rho) = \rho, \ \mathcal{F}\mathcal{E}(\sigma) = \sigma.$$

An explicit form of $\mathcal{F}$ is, see (Hayden *et al.*, 2004),

$$\mathcal{F}(\tau) = \sigma^{1/2}\mathcal{E}^{\dagger}((\mathcal{E}(\sigma))^{-1/2}\tau(\mathcal{E}(\sigma))^{-1/2})\sigma^{1/2}, \ \tau \in \mathcal{S}(K). \tag{42}$$

Apply (41) to (40), we know there exists an operator $\mathcal{F}^{a_1 b}$ such that

$$\mathcal{F}^{a_1 b}(\mathcal{T}_{a_2}^{a_1 a_2}\mathcal{E}^a \otimes \mathcal{I}^b)(\rho^{ab}) = \rho^{ab},$$

$$\mathcal{F}^{a_1 b}(\mathcal{T}_{a_2}^{a_1 a_2}\mathcal{E}^a \otimes \mathcal{I}^b)(\rho^a \otimes \rho^b) = \rho^a \otimes \rho^b.$$

Consider the explicit form of $\mathcal{F}^{a_1 b}$ from (42) and the product structure of $\rho^a \otimes \rho^b$, we can express $\mathcal{F}^{a_1 b}$ as $\mathcal{F}^{a_1} \otimes \mathcal{I}^b$, hence

$$(\mathcal{F}^{a_1} \otimes \mathcal{I}^b)(\mathcal{T}_{a_2}^{a_1 a_2}\mathcal{E}^a \otimes \mathcal{I}^b)(\rho^{ab}) = \rho^{ab}$$

Use Lemma 1, we obtain

$$\rho^{ab} = \sum_i X_i^a \otimes X_i^b,$$

where X_i^a is non-negative, $\{X_i^b\}$ constitutes a linearly independent set, thus

$$\sum_i \mathcal{F}^{a_1}\mathcal{T}_{a_2}^{a_1 a_2}\mathcal{E}^a(X_i^a) \otimes X_i^b = \sum_i X_i^a \otimes X_i^b,$$

since $\{X_i^b\}$ is a linearly independent set, we have

$$\mathcal{F}^{a_1}\mathcal{T}_{a_2}^{a_1 a_2}\mathcal{E}^a(X_k^a) = X_k^a, \ \forall k.$$

So $\{X_i^a\}$ is broadcastable, due to Theorem 1, X_i^a's commute with each other, and hence can be diagonalized by the same basis $\{|i\rangle\}$, now we obtain

$$\rho^{ab} = \sum_i \lambda_i |i\rangle\langle i| \otimes Y_i^b,$$

it can be easily proved that Y_i^b is non-negative, and hence ρ^{ab} is indeed a classical-quantum state.

Now we prove Theorem 3 $\Rightarrow$ Theorem 2.

Proof: We shall prove only the non-trivial part. Suppose the correlation in ρ^{ab} can be locally broadcast by two operators respectively performed on party a and b:

$$\begin{aligned}\mathcal{E}^a &: \mathcal{S}(H^a) \to \mathcal{S}(H^{a_1} \otimes H^{a_2}),\\ \mathcal{E}^b &: \mathcal{S}(H^b) \to \mathcal{S}(H^{b_1} \otimes H^{b_2}),\end{aligned}$$

then we obtain

$$\begin{aligned}\rho^{a_1 a_2 b_1 b_2} &= (\mathcal{E}^a \otimes \mathcal{E}^b)\rho^{ab}\\ &= (\mathcal{I}^{a_1 a_2} \otimes \mathcal{E}^b)(\mathcal{E}^a \otimes \mathcal{I}^b)\rho^{ab}.\end{aligned}$$

So we have decomposed the operation $\mathcal{E}^a \otimes \mathcal{E}^b$ into two steps, each of which only deals with a single party. Through step one, we obtain

$$S(\rho^{ab}|(\rho^a \otimes \rho^b)) \geq S(\mathcal{E}^a(\rho^{ab})|\mathcal{E}^a(\rho^a \otimes \rho^b)),$$

that is, $I(\rho^{ab}) \geq I(\rho^{a_1 a_2 b})$, since $I(\rho^{a_1 a_2 b}) \geq I(\mathrm{Tr}_{a_2}\rho^{a_1 a_2 b}) = I(\rho^{a_1 b})$, we have

$$I(\rho^{a_1 b}) \leq I(\rho^{a_1 a_2 b}) \leq I(\rho^{ab}).$$

Similarly, through step two, we obtain

$$I(\rho^{a_1b_1}) \le I(\rho^{\rho^{a_1b_1b_2}}) \le I(\rho^{a_1b}).$$

With the condition $I(\rho^{a_1b_1}) = I(\rho^{ab})$, we have $I(\rho^{a_1b}) = I(\rho^{ab})$, which shows that the correlation in ρ^{ab} is broadcast by party a, from Theorem 3, we know ρ^{ab} is a classical-quantum state. Exchange a and b in the above discussion, it's obvious that ρ^{ab} is also a quantum-classical state. So ρ^{ab} is a classical state.

Next we prove Theorem 2 ⇒ Theorem 1

Proof: Again we shall only prove the non-trivial part. Suppose there exists a quantum operation $\mathcal{E}^b$ which can broadcast a set of states $\{\rho_i^b\}$. We can find a orthonormal set $\{|i\rangle\}$ and construct a composite system

$$\rho^{ab} = \sum_i p_i|i\rangle\langle i| \otimes \rho_i^b,$$

where $\{p_i\}$ is a probability distribution. The party a can be easily broadcast by the operator $\mathcal{E}^a$ form (39), together with $\mathcal{E}^b$, ρ^{ab} can be locally broadcast, so is the correlation. Thus from Theorem 2, ρ^{ab} is a classical state, then ρ_i^b commutes with each other.

From the above discussions, we have created a chain of equivalence among the three theorems: Theorem 1 ⇔ Theorem 2 ⇔ Theorem 3. This has provided us with a unified picture of the no-broadcasting theorem in quantum systems from the information theoretical point of view.

E. No-cloning and no-signaling

According to Einstein's relativity theory, superluminal signaling cannot be physically realized. Yet due to the non-local property of quantum entanglement, superluminal signaling is possible provided perfect cloning machine can be made. The scheme has been well-known since Herbert(Herbert, 1982) first proposed his "FLASH" in 1982. The idea is as follows: suppose Alice and Bob, at an arbitrary distance, share a pair of entangled qubits in the state $|\psi\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)$. Alice can measure her qubit by either σ_x or σ_z. If the measurement is σ_z, Alice's qubit will collapse to the state $|0\rangle$ or $|1\rangle$, with probability 50%. Respectively, this prepares Bob's qubit in the state $|1\rangle$ or $|0\rangle$. Without knowing the result of Alice's measurement, the density matrix of Bob's qubit is $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}I$. On the other hand, if Alice's measurement is σ_x, Alice's qubit will collapse to the state $|\varphi_{x+}\rangle$ or $|\varphi_{x-}\rangle$, where $|\varphi_{x+}\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$, $|\varphi_{x-}\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$, being eigenvectors of σ_x. Thus Bob's qubit is prepared in the state $|\varphi_{x-}\rangle$ or $|\varphi_{x+}\rangle$ respectively, in this case the density matrix of Bob's qubit is still $\frac{1}{2}|\varphi_{x+}\rangle\langle\varphi_{x+}| + \frac{1}{2}|\varphi_{x-}\rangle\langle\varphi_{x-}| = \frac{1}{2}I$. Obviously, Bob gets no information about which measurement is made by Alice. While, if perfect cloning is allowed, the scenario will change. Bob can use the cloning machine to make arbitrarily many copies of his qubit, in which way he is able to determine the exact state of his qubit, that is, whether an eigenstate of σ_z or σ_x. With this information, Bob knows the measurement Alice has taken. Fortunately, since no-cloning theorem has been proved, the above superluminal signaling scheme cannot be realized, which leaves theory of relativity and quantum mechanics in coexistence.

Up to now, there are many cloning schemes found, naturally one may ask, whether it is possible by using imperfect cloning, to extract information about which measuring basis Alice has used. According to the property of quantum transformation, the answer is no. To see this, we may first consider a simple scheme, that is, Bob can use the universal quantum cloning machine (UQCM) proposed by Bužek and Hillery(Bužek and Hillery, 1996) to process his qubit. The UQCM transformation reads,

$$|0\rangle|Q\rangle \to \sqrt{\frac{2}{3}}|00\rangle|\uparrow\rangle + \sqrt{\frac{1}{3}}|+\rangle|\downarrow\rangle,$$

$$|1\rangle|Q\rangle \to \sqrt{\frac{2}{3}}|11\rangle|\downarrow\rangle + \sqrt{\frac{1}{3}}|+\rangle|\uparrow\rangle,$$

where $|Q\rangle$ is the original state of the copying-machine, $|+\rangle$ and $|-\rangle$ are two orthogonal states of the output, $|+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, and $|\uparrow\rangle, |\downarrow\rangle$ are the ancillary states which are orthogonal to each other. If Alice chooses σ_z, the density matrix of Bob's qubit after the process is

$$\begin{aligned}\rho_b &= \frac{1}{2}(\frac{2}{3}|00\rangle\langle 00| + \frac{1}{3}|+\rangle\langle +|) + \frac{1}{2}(\frac{2}{3}|11\rangle\langle 11| + \frac{1}{3}|+\rangle\langle +|)\\ &= \frac{1}{3}(|00\rangle\langle 00| + |11\rangle\langle 11| + |+\rangle\langle +|).\end{aligned}$$

If Alice chooses σ_x, it can be easily verified that the density matrix will not change, thus no information can be gained by Bob. In fact, Bruss *et al.* have pointed out in (Bruß *et al.*, 2000b) that the density matrix of Bob's qubit will not change no matter what operation is taken on it, as long as the operation is linear and trace-preserving. Suppose the original density matrix shared between Alice and Bob is ρ^{ab}, and Alice has done a measurement $\mathcal{A}_m$ on her qubit, Bob makes a transformation $\mathcal{B}$ on his, then the shared density matrix becomes $\mathcal{A}_m \otimes \mathcal{B}(\rho^{ab})$, here m specifies which measurement Alice has taken. In Bob's view, with the linear and trace-preserving property of $\mathcal{A}_m$, the density matrix of his qubit is

$$\begin{aligned} tr_a(\mathcal{A}_m \otimes \mathcal{B}(\rho^{ab})) &= \mathcal{B} tr_a(\mathcal{A}_m \otimes \mathcal{I}(\rho^{ab})) \\ &= \mathcal{B} tr_a(\rho^{ab}). \end{aligned}$$

Note that tr and Tr both denote trace similarly in this review. Here we see that the density matrix of Bob's qubit has nothing to do with Alice's measurement $\mathcal{A}_m$, therefore no information is transferred to Bob. Note that to get the above conclusion, we have only used the linear and trace-preserving property of $\mathcal{A}_m$. Since any quantum operator is linear and completely positive, no-signaling should always hold, thus providing a method to determine the fidelity limit of a cloning machine.

Gisin studied the case of $1 \to 2$ qubit UQCM in (Gisin, 1998). We continue the scheme that Alice and Bob share a pair of entangled states. Now Alice has done some measurement by σ_x or σ_z, and thus Bob's state has been prepared in a respect mixed state. Let there be a UQCM, suppose the input density matrix is $|\varphi\rangle\langle\varphi| = \frac{1}{2}(I + \boldsymbol{m} \cdot \boldsymbol{\sigma})$, with $\boldsymbol{m}$ being the Bloch vector of $|\varphi\rangle$, then after cloning the reduced state on party a and b should read, $\rho^a = \rho^b = (1+\eta \boldsymbol{m} \cdot \boldsymbol{\sigma})$, yielding the fidelity to be $F = (1+\eta)/2$. According to the form of ρ^a and ρ^b, the composite output state of the cloning machine should be

$$\rho^{out} = \frac{1}{4}(I_4 + \eta(\boldsymbol{m} \cdot \boldsymbol{\sigma} \otimes I + I \otimes \boldsymbol{m} \cdot \boldsymbol{\sigma}) + \sum_{i,j=x,y,z} t_{ij} \sigma_i \otimes \sigma_j).$$

The universality of UQCM requires

$$\rho_{out}(U\boldsymbol{m}) = U \otimes U \rho_{out}(\boldsymbol{m}) U^{\dagger} \otimes U^{\dagger}. \tag{43}$$

The no-signaling condition requires

$$\frac{1}{2}\rho^{out}(+x) + \frac{1}{2}\rho^{out}(-x) = \frac{1}{2}\rho^{out}(+z) + \frac{1}{2}\rho^{out}(-z), \tag{44}$$

where $\rho^{out}(+z)$ represents the output state of the UQCM under the condition that Alice has take the measurement σ_x and got result $+$.

Also we should notice that ρ^{out} must be positive. Putting the positive condition together with (43) and (44), we shall get $\eta \leq \frac{2}{3}(F \leq \frac{5}{6})$. Although we have found an upper bound of F, the question remains whether it can be reached. But we know it can be, since a practical UQCM scheme with $F = \frac{5}{6}$ has been proposed(Bužek and Hillery, 1996).

Navez *et al.* have derived the upper bound of fidelity for d-dimensional $1 \to 2$ UQCM using no-signaling condition(Navez and Cerf, 2003), and the bound also has been proved to be tight. Simon *et al.* have shown how no-signaling condition together with the static property of quantum mechanics can lead to properties of quantum dynamics (Simon *et al.*, 2001). By static properties we mean: 1) The states of quantum systems are described as vectors in Hilbert space. 2) The usual observables are represented by projections in Hilbert space and the probabilities for measurement are described by the usual trace rule. The two properties with no-signaling condition shall imply that any quantum map must be completely positive and linear, which is what we already have in mind. This may help to understand why bound derived by no-signaling condition is always tight. The experimental test of the no-signaling theorem is also performed in optical system (De Angelis *et al.*, 2007). From no-signaling condition, the monogamy relation of violation of Bell inequalities can be derived, and this can be used to obtain the optimal fidelity for asymmetric cloning (Pawlowski and Brukner, 2009). And some general properties of no-signaling theorem are presented in (Masanes *et al.*, 2006). The relationship between optimal cloning and no signaling is presented in (Ghosh *et al.*, 1999). The no-signaling is shown to be related with optimal state estimation (Han *et al.*, 2010). Also the no-signaling is equivalent to the optimal condition in minimum-error quantum state discrimination (Bae *et al.*, 2011), more results of those topics can be found in (Bae and Hwang, 2012) for qubit case and (Bae, 2012b) for the general case. The optimal cloning of arbitrary fidelity by using no-signaling is studied in (Gedik and Çakmak, 2012).

F. No-cloning for unitary operators

No-cloning is a fundamental theorem in quantum information science and quantum mechanics. It may be manifested in various versions. Simply by calculation, and with the help of definition of CNOT gate, we may find the following relations,

$$
\begin{aligned}
CNOT(\sigma_x \otimes I)CNOT &= \sigma_x \otimes \sigma_x, \\
CNOT(\sigma_z \otimes I)CNOT &= \sigma_z \otimes I, \\
CNOT(I \otimes \sigma_x)CNOT &= I \otimes \sigma_x, \\
CNOT(I \otimes \sigma_z)CNOT &= \sigma_z \otimes \sigma_z.
\end{aligned} \tag{45}
$$

It implies that the bit flip operation is copied forwards (from first qubit to second qubit), while the phase flip operation is copied backwards. But we cannot copy simultaneously the bit flip operation and phase flip operation. Those properties are important for methods of quantum error correction and fault-tolerant quantum computation (Gottesman, 1998). This is a kind of no-cloning theorem for unitary operators. The quantum cloning of unitary operators is investigated in (Chiribella *et al.*, 2008).

G. Other developments and related topics

One important application of quantum information science is the quantum key distribution for quantum cryptography, which can provide the unconditional security for secrete key sharing. The security of the quantum key distribution is based on no-cloning theorem since if we can copy perfectly the transferred state, we can always find its exact form by copying it to infinite copies so that its exact form can be found. For quantum cryptography protocol E91 (Ekert, 1991), the security is based on the violation of Bell inequality (Bell, 1964). The unified picture of no-broadcasting theorem unifies those theorems together. This is also shown in (Acín *et al.*, 2004a). The no-cloning theorem for entangled states is shown in (Koashi and Imoto, 1998). Related with entanglement cloning, it is also shown that orthogonal states in composite systems cannot be cloned (Mor, 1998), related results are also available in (Goldenberg and Vaidman, 1996; Peres, 1996a). On the other hand, as a reverse process of quantum cloning, it is also pointed out that it is impossible to delete an unknown quantum state (Pati and Braunstein, 2000). Quantum no-broadcasting can also be related with bounds on quantum capacity (Janzing and Steudel, 2007). Different from quantum case, classical broadcasting is possible with arbitrary high resolution (Walker and Braunstein, 2007). The difference between quantum copying and classical copying is studied in (Shen *et al.*, 2011), see also (Fenyes, 2012). The classical no-cloning is also discussed (Daffertshofer *et al.*, 2002). The linear assignment maps for correlated system-environment states is studied in (Rodriguez-Rosario *et al.*, 2010), the connection between the violation of the positivity of this linear assignments and the no-broadcasting theorem is found. By studying quantum correlation different from quantum entanglement, the equivalence between locally broadcastable and broadcastable is investigated in (Wu and Guo, 2011), see a review about quantumness of correlations (Modi *et al.*, 2012). The no-signaling principle and the state distinguishability is studied in (Bae, 2012a). The transformations which preserve commutativity of quantum states are studied in (Nagy, 2009). The quantum channels related with quantum cloning are studied in (Bradler, 2011). It is also pointed out that no-cloning of non-orthogonal states does not necessarily mean that inner product of quantum states should preserve (Li *et al.*, 2005b). No-cloning theorem means that two copies cannot be obtained out of a single copy, and if we study the information content measured by Holevo quantity of one copy and two copies, a condition of states broadcasting can be obtained (Horodecki *et al.*, 2006). It is also shown that no-cloning theorem is, in principle, equivalent with no-increasing of entanglement (Horodecki and Horodecki, 1998). The impossibility of reversing or complementing an unknown quantum state is a generalization of no-cloning theorem (Li *et al.*, 2005a). The no-cloning studied by wave-packet collapse of quantum measurement is presented by Luo in (Luo, 2010a).

No-cloning theorem is also illustrated in (Dieks, 1982; Wootters and Zurek, 2009; Yuen, 1986), it is also related with the no-imprinting theorem (Bennett *et al.*, 1992), see related results in (Koashi and Imoto, 2002). The geometrical interpretation of no-cloning theorem is proposed as quantum no-stretching (D'Ariano and Perinotti, 2009). It is shown that quantum information cannot be split into complementary parts, this is no-splitting (Zhou *et al.*, 2006). The combination of no-cloning, no-broadcasting and monogamy of entanglement can be found in (Leifer, 2006). The application of quantum cloning in quantum computation is discussed in (Galvao and Hardy, 2000).

III. UNIVERSAL QUANTUM CLONING MACHINES

As we have shown in last section, there are various no-cloning theorems implied by the law of quantum mechanics. They imply that one cannot clone an arbitrary qubit perfectly. On the other hand, the approximate quantum cloning is not prohibited. So it is possible that one can get several copies that approximate the original state, with fidelity $F < 1$. Hence one naturally raises a question: can we achieve the same fidelity for any state on the Bloch sphere, for the qubit case, or more generally, for any state in a d-dimensional Hilbert space? And what is the best fidelity we can get?

A cloning machine that achieves equal fidelity for every state is called a universal quantum cloning machine (UQCM). This problem is equivalent to distribute information to different receivers, and it is natural to require the performance is the same for every input state, since we do not have any specific information about the input state ahead. According to no-cloning theorem, it is expected that the original input state will be destroyed and become as one of the output copies. For the simplest case, one qubit is cloned to have two copies, those two copies can be identical to each other, i.e., they are symmetric and of course they are different from the original input state. On the other hand, those two copies can also be different, both of them are similar to the the original input state but with different similarities, we mean that they are asymmetric. In this sense, there are symmetric and asymmetric UQCMs.

A. Symmetric UQCM for qubit

Consider a quantum cloning from 1 qubit to 2 qubits, a trivial scheme can be simply constructed as following:

(1), Measure the input state $|\vec{a}\rangle$ in a random base $|\vec{b}\rangle$. Here the vectors are on the Bloch sphere S^2. The probability of obtaining result $|\pm\vec{b}\rangle$ is $p_\pm = \left(1 \pm \vec{a}\cdot\vec{b}\right)/2$.

(2), Then duplicate the state $|\pm\vec{b}\rangle$ according to the measurement result. The fidelity is $F_+ = |\langle\vec{a}|+\vec{b}\rangle|^2$ and $F_- = |\langle\vec{a}|-\vec{b}\rangle|^2$, respectively.

In an average sense, the fidelity is

$$F_{trivial} = \int_{S^2} p_+F_+ + p_-F_- = \frac{1}{2} + \frac{1}{2}\int_{S^2}\left(\vec{a}\cdot\vec{b}\right)^2 \mathrm{d}\vec{b} = \frac{2}{3}. \tag{46}$$

The problem is: can we design a better cloning machine? Bužek and Hillery (Bužek and Hillery, 1996) proposed an optimal UQCM, namely, a unitary transformation on a larger Hilbert space:

$$U|0\rangle_1|0\rangle_2|0\rangle_R = \sqrt{\frac{2}{3}}|0\rangle_1|0\rangle_2|0\rangle_R + \sqrt{\frac{1}{6}}(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2)|1\rangle_R, \tag{47}$$

$$U|1\rangle_1|0\rangle_2|0\rangle_R = \sqrt{\frac{2}{3}}|1\rangle_1|1\rangle_2|1\rangle_R + \sqrt{\frac{1}{6}}(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2)|0\rangle_R. \tag{48}$$

On the l.h.s of the equations, the first qubit 1 is the input state, the second is a blank state and the third with subindex R is the ancillary state of the quantum cloning machine itself. By a unitary transformation which is demanded by quantum mechanics, we find the output state on the r.h.s. of the equations. We may find that the original qubit is destroyed and becomes as one of the output qubit in 1 while the blank state is now changed as another copy in party 2, the ancillary state R may or may not be changed which will be traced out for the output. It is obvious that two output states are identical, so it is a symmetric quantum cloning machine.

For an arbitrary normalized pure input state $|\psi\rangle = a|0\rangle + b|1\rangle$, since quantum mechanics is linear, by applying U on the state which is realized simply by following the above cloning transformation, we can find the copies. After tracing out the ancillary state, the output density matrix take the form:

$$\rho_{out} = \frac{2}{3}|\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi| + \frac{1}{6}(|\psi\rangle|\psi^\perp\rangle + |\psi^\perp\rangle|\psi\rangle)(\langle\psi|\langle\psi^\perp| + \langle\psi^\perp|\langle\psi|). \tag{49}$$

Here $|\psi^\perp\rangle = b^*|0\rangle - a^*|1\rangle$ is orthogonal to $|\psi\rangle$. We can further trace out one of the two states to get the single copy density matrix

$$\rho_1 = \rho_2 = \frac{2}{3}|\psi\rangle\langle\psi| + \frac{1}{6}I. \tag{50}$$

Note this density matrix is of the form $\eta|\psi\rangle\langle\psi| + \frac{1-\eta}{d}I$ with η called the "shrinking factor". This form is a linear combination of the original density matrix $|\psi\rangle\langle\psi|$ and the identity I which corresponds to completely mixed state and it is like a white noise.

In fact, in the original papers, the efficiency of the cloning machine is described by Hilbert-Schmidt norm $d_{HS}^2 = \mathrm{Tr}[(\rho_{in}-\rho_{out})^\dagger(\rho_{in}-\rho_{out})]$, which also quantifies the distance of two quantum states. The fidelity is a general accepted measure of merit of the quantum cloning (Kwek *et al.*, 2000). We will generally use fidelity as the measure of the quality of the copies in this review.

We can obtain the single copy fidelity

$$F_1 = \langle\psi|\rho_1|\psi\rangle = \frac{5}{6}, \tag{51}$$

and the two copies fidelity (global fidelity),

$$F_2 =^{\otimes 2} \langle\psi|\rho_1|\psi\rangle^{\otimes 2} = \frac{2}{3}. \tag{52}$$

The single copy fidelity provides measure of similarity between state ρ_1 and the original input state. If it is one, those two states are completely the same, while if it is zero, those two states are orthogonal. One point may be noticed is that, the fidelity between a completely mixed state with $|\psi\rangle$ is $1/2$. We know that a completely mixed state contains nothing about the input state, so fidelity $1/2$ should be the farthest distance between two quantum states. Similarly, the global fidelity quantifies the similarity between the two-qubit output state with the ideal cloning case. If it is one, we have two perfect copies. We remark that the single copy fidelity does not depend on input state, so the quality of the copies has the state-independent characteristic. In this sense, the corresponding cloning machine is "universal". One may find that the above presented cloning machine achieves higher fidelity than the trivial one, and it is proved to be optimal (Bruß *et al.*, 1998a; Gisin, 1998; Gisin and Massar, 1997)).

Gisin and Massar (Gisin and Massar, 1997) then generalize the cloning machine to $N \to M$ case, that is M copies are created from N identical qubits. Their cloning machine is a transformation:

$$|N\psi\rangle|R\rangle \to \sum_{j=0}^{M-N} \alpha_j |(M-j)\psi, j\psi^\perp\rangle|R_j\rangle \tag{53}$$

where

$$\alpha_j = \sqrt{\frac{N+1}{M+1}}\sqrt{\frac{(M-N)!(M-j)!}{(M-N-j)!M!}} \tag{54}$$

and$|(M-j)\psi, j\psi^\perp\rangle$ denote the normalized symmetric state with $M-j$ states $|\psi\rangle$ and j states $|\psi^\perp\rangle$. Then the single copy fidelity is

$$F = \frac{M(N+1)+N}{M(N+2)}. \tag{55}$$

In (Gisin and Massar, 1997) the optimality of this cloning machine is proved for cases $N = 1, 2, \ldots, 7$. The complete proof of the optimality is finished in (Bruß *et al.*, 1998b) where the connection between optimal quantum cloning and optimal state estimation is established. The upper bound of N to M UQCM is found to be exactly equal to (55), hence Gisin and Massar UQCM is optimal.

B. Symmetric UQCM for qudit

For further generalization, we may seek cloning machine for d-level systems. Bužek and Hillery proposed a 1 to 2 d-dimensional UQCM (Bužek and Hillery, 1999)(Bužek and Hillery, 1998): for a basis state $|i\rangle$, the transformation is

$$|i\rangle|0\rangle|R\rangle \to \frac{2}{\sqrt{2(d+1)}}|i\rangle|i\rangle|R_i\rangle + \frac{1}{\sqrt{2(d+1)}}\sum_{i\neq j}(|i\rangle|j\rangle + |j\rangle|i\rangle)|R_j\rangle. \tag{56}$$

Here $|R_i\rangle$ is a set of orthogonal normalized ancillary state. The resultant one copy fidelity is, $F = (d+3)/(2d+2)$.

Later, a general N to M UQCM is constructed in a concise way by Werner (Werner, 1998), see also (Zanardi, 1998) for related results. For N identical pure input state $|\psi\rangle$, the output density matrix is:

$$\rho_{out} = \frac{d[N]}{d[M]} s_M \left((|\psi\rangle\langle\psi|)^{\otimes N} \otimes I^{\otimes(M-N)} \right) s_M \tag{57}$$

where $d[N]=\binom{d+N-1}{N}$, (we also use notation $d[N]=C^N_{d+N-1}$), and s_M is a symmetrization operator that maps state in $\mathcal{H}^{\otimes M}$ to symmetric state in the symmetric Hilbert space $\mathcal{H}_+^{\otimes M}$. As an example,

$$s_2=|00\rangle\langle 00|+|11\rangle\langle 11|+\frac{1}{2}(|01\rangle+|10\rangle)(\langle 01|+\langle 10|). \tag{58}$$

If we insert this expression into formula (57), we can get exactly the expression of output density matrix (49). So this UQCM can recover the $N=1$, $M=2$, $d=2$ one.

For N to M case, the single copy fidelity is shown to be

$$\begin{aligned} F_1 &= \frac{d[N]}{d[M]}\mathrm{Tr}\left[\left(|\psi\rangle\langle\psi|\otimes I^{\otimes(M-1)}\right)s_M\left((|\psi\rangle\langle\psi|)^{\otimes N}\otimes I^{\otimes(M-N)}\right)s_M\right] \\ &= \frac{N(M+d)+M-N}{M(N+d)}. \end{aligned} \tag{59}$$

In (Werner, 1998), this single copy fidelity is proved to be optimal under the restriction that the operation is a mapping into the symmetric Hilbert space. Generally, there might exist a cloning machine performing better without this constraint. Keyl and Werner studied the more general case and proved this cloning machine is indeed the unique optimal UQCM (Keyl and Werner, 1999). As a special case, if we let $N=1$, $M=2$, the fidelity apparently reduces to the Bužek and Hillery 1 to 2 d-dimensional UQCM: $F=(d+3)/(2d+2)$. And if we take the $M\to\infty$ limit, the fidelity turns out to be $F=(N+1)/(N+d)$, this agrees with the state estimation result by Massar and Popescu (Massar and Popescu, 1995).

We are also interested in the M copies fidelity (global fidelity), it can be found as follows (Werner, 1998),

$$\begin{aligned} F_M &= \frac{d[N]}{d[M]}tr\left[(|\psi\rangle\langle\psi|)^{\otimes M}s_M\left((|\psi\rangle\langle\psi|)^{\otimes N}\otimes I^{\otimes(M-N)}\right)s_M\right] \\ &= \frac{d[N]}{d[M]}tr\left((|\psi\rangle\langle\psi|)^{\otimes M}\right) \\ &= \frac{d[N]}{d[M]}=\frac{M!(N+d-1)!}{N!(M+d-1)!}. \end{aligned} \tag{60}$$

Recently, Wang *et al.* (Wang *et al.*, 2011b) proposed a more general definition "L copies fidelity": $F_L={}^{\otimes L}\langle\psi|\rho_{out,L}|\psi\rangle^{\otimes L}$ where $\rho_{out,L}$ is the L copies output reduced density matrix. The expression is calculated as,

$$F_L=\frac{(d+N-1)!(M-N)!(M-L)!}{(d+M-1)!M!N!}\times\sum_{m_1}\frac{(M-m_1+d-2)!(m_1!)^2}{(m_1-L)!(m_1-N)!(d-2)!(M-m_1)!}. \tag{61}$$

For $L=1$ and $L=M$, the expression will reduce to results presented above (59,60). For another special case $N=1$, expression of fidelity can be simplified by finding the explicit result of the summation, it reads,

$$F_L(N=1)=\frac{L!d![L(d+M)+M-L]}{(d+L)!M}. \tag{62}$$

Fan *et al.* (Fan *et al.*, 2001a) proposed another version of UQCM, written in more explicit form: let $\boldsymbol{n}=(n_1,\ldots,n_d)$ denote a d-component vector. And $|\boldsymbol{n}\rangle=|n_1,\ldots,n_d\rangle$ is a completely symmetric and normalized state with n_i states in $|i\rangle$. These states is an orthogonal normalized basis of the symmetric Hilbert space $\mathcal{H}_+^{\otimes M}$. Then for an arbitrary input state $|\psi\rangle=\sum_{i=1}^d x_i|i\rangle$, the N-fold direct product $|\psi\rangle^{\otimes N}$ could be expanded as:

$$|\psi\rangle^{\otimes N}=\sum_{\boldsymbol{n}}^{N}\sqrt{\frac{N!}{n_1!\ldots n_d!}}x_1^{n_1}\ldots x_d^{n_d}|\boldsymbol{n}\rangle. \tag{63}$$

The cloning transformation takes the form,

$$|\boldsymbol{n}\rangle|R\rangle\to\sum_{\boldsymbol{j}}^{M-N}\alpha_{\boldsymbol{nj}}|\boldsymbol{n}+\boldsymbol{j}\rangle|R_{\boldsymbol{j}}\rangle \tag{64}$$

The notation $\sum_{\boldsymbol{n}}^{N}$ means summation over all possible vectors $\boldsymbol{n}$ with $n_1 + \cdots + n_d = N$ and the $|R_{\boldsymbol{j}}\rangle$ is a set of orthogonal normalized ancillary states, as usual. The coefficients $\alpha_{\boldsymbol{nj}}$ are:

$$\alpha_{\boldsymbol{nj}} = \sqrt{\frac{(M-N)!(N+d-1)!}{(M+d-1)!}}\sqrt{\prod_{k=1}^{d}\frac{(n_k+j_k)!}{n_k!j_k!}}. \tag{65}$$

This UQCM can achieve the same fidelities as the UQCM given by Werner (Werner, 1998). It is optimal. Later Wang *et al.* (Wang *et al.*, 2011b) proved that these two cloning machines are indeed equivalent by showing the output states are the same. First, divide the symmetric state $|\vec{m}\rangle$ of M qudits into two parts with N qudits and $M-N$ qudits, respectively,

$$|\vec{m}\rangle = \frac{1}{\sqrt{C_M^N}}\sum_{\vec{k}}^{M-N}\prod_j\sqrt{\frac{m_j!}{(m_j-k_j)!k_j!}}|\vec{m}-\vec{k}\rangle|\vec{k}\rangle. \tag{66}$$

The symmetry operator s_M can be reformulated. After calculation, output density matrix in (57) is shown to be:

$$\rho_{out} = \frac{N!(M-N)!(N+d-1)!}{(M+d-1)!}\sum_{\vec{m},\vec{m}'}^{M}|\vec{m}\rangle\langle\vec{m}'| \times \left(\sum_{\vec{k}}^{M-N}\prod_j\frac{x_j^{m_j-k_j}x^{*(m_j'-k_j)}\sqrt{m_j!m_j'!}}{(m_j-k_j)!(m_j'-k_j)!k_j!}\right). \tag{67}$$

For the cloning machine (64), we can get the output density matrix after tracing out the ancillary state:

$$\rho'^{out} = \frac{N!(M-N)!(N+d-1)!}{(M+d-1)!}\eta^2\sum_{\vec{n},\vec{n}'}^{N}\sum_{\vec{k}}^{M-N}|\vec{n}+\vec{k}\rangle\langle\vec{n}'+\vec{k}| \times \left(\prod_j\frac{x_j^{n_j}x_j^{*(n_j')}\sqrt{(n_j+k_j)!(n_j'+k_j)!}}{n_j!n_j'!k_j!}\right). \tag{68}$$

These two expressions are apparently equivalent.

In (Wang *et al.*, 2011b), a unified form of the symmetric UQCM is presented, up to an unimportant overall normalization factor, the transformation is,

$$|\psi\rangle^{\otimes N}|\Phi^+\rangle^{\otimes(M-N)} \to \left(s_M \otimes I^{\otimes(M-N)} \otimes I^{\otimes N}\right)|\psi\rangle^{\otimes N}|\Phi^+\rangle^{\otimes(M-N)}. \tag{69}$$

This cloning machine is realized by superposition of states in which some of the input states are permutated into one part of the maximally entangled states. Since $s_M = s_M(I^{\otimes N}\otimes s_{M-N})$, and the mapping of s_{M-N} on the $M-N$ maximally entangled states is: $(s_{M-N}\otimes I^{M-N})|\Phi^+\rangle^{\otimes(M-N)}$, the cloning transformation may be rewritten as:

$$\begin{aligned}
&\left(s_M \otimes I^{\otimes(M-N)}\right)|\vec{n}\rangle|\Phi^+\rangle^{\otimes(M-N)} \\
&= \left(s_M \otimes I^{\otimes(M-N)}\right)|\vec{n}\rangle\sum_{\vec{k}}^{M-N}|\vec{k}\rangle|\vec{k}\rangle \\
&= \sum_{\vec{k}}^{M-N}\sqrt{\prod_j\frac{(n_j+k_j)!}{n_j!k_j!}}|\vec{n}+\vec{k}\rangle|\vec{k}\rangle.
\end{aligned} \tag{70}$$

In fact this coincides with the UQCM (64). Here the complicated coefficients (65) proposed for optimal cloning machine can be naturally obtained. Also it can be simply seen that the transformation (69) is equivalent to the construction (57) if the ancillary states are traced out. So the UQCM can be simply constructed, we can symmetrize the N input pure states and halves of some maximally entangled states, while other halves of the maximally entangled states are ancillary states. This simplify dramatically the construction of the UQCM theoretically and its physical implementation becomes easier. If maximally entangled states are available, the UQCM is to symmetrize the input pure states with one sides of the maximally entangled states. Indeed, some experiments follow this scheme.

C. Asymmetric quantum cloning

In the previous subsections we are considering symmetric cloning machines which provide identical output copies. However, naturally we may try to distribute information unequally among the copies. The 1 to 2 optimal asymmetric qubit cloner is found by Niu and Griffiths (Cerf, 2000b), Cerf (Niu and Griffiths, 1998) and Bužek, Hillery and Bednik(Bužek *et al.*, 1998). Their formalisms are slightly different, but they lead to a same relation between A's fidelity F_A and B's fidelity F_B:

$$\sqrt{(1-F_A)(1-F_B)} \geq F_A + F_B - \frac{3}{2} \tag{71}$$

So a tradeoff relation exists for the two fidelities, if one fidelity is large, correspondingly another fidelity will become small. This will be presented further in the following.

The transformation can be written in the following form according to Bužek *et al.*(Bužek *et al.*, 1998):

$$|\psi\rangle_A(a|\Phi^+\rangle_{BR} + b|0\rangle_B(|0\rangle_R + |1\rangle_R)/\sqrt{2}) \rightarrow a|\psi\rangle_A|\Phi^+\rangle_{BR} + b|\psi\rangle_B|\Phi^+\rangle_{AR} \tag{72}$$

Here R is an ancillary state, $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ is a Bell basis. And the normalization condition of input state requires $a^2 + ab + b^2 = 1$, which is an ellipse equation. The reduced density matrix of A and B are: $\rho_{A,B} = F_{A,B}|\psi\rangle\langle\psi| + (1-F_{A,B})|\psi^\perp\rangle\langle\psi^\perp|$, here

$$F_A = 1 - b^2/2, F_B = 1 - a^2/2, \tag{73}$$

which is just the fidelity of A and B, respectively. It is easy to check (73) satisfy the inequality (71). And as special cases, we can see if a=0, then $F_A = 1$, $F_B = 1/2$, hence the information all goes to A, and for B it's all the same. If $a^2 = b^2 = 1/3$, then it reduces to symmetric UQCM case, with fidelity $F_A = F_B = 5/6$.

For completeness, here we would like to present a slightly different form for the asymmetric quantum cloning which is named by Cerf as a Pauli channel(Cerf, 2000b). We start from qubit case. An arbitrary quantum pure state takes the form,

$$|\psi\rangle = x_0|0\rangle + x_1|1\rangle, \quad \sum_j |x_j|^2 = 1. \tag{74}$$

A maximally entangled state is written as

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{75}$$

We can write the complete quantum state of three particles as

$$\begin{aligned} |\psi\rangle_A|\Psi^+\rangle_{BC} &= \frac{1}{2}[|\Psi^+\rangle_{AB}|\psi\rangle_C \\ &+(I\otimes X)|\Psi^+\rangle_{AB}X|\psi\rangle_C \\ &+(I\otimes Z)|\Psi^+\rangle_{AB}Z|\psi\rangle_C \\ &+(I\otimes XZ)|\Psi^+\rangle_{AB}XZ|\psi\rangle_C], \end{aligned} \tag{76}$$

where I is the identity, X, Z are two Pauli matrices and XZ is another Pauli matrix up to a whole factor i.

Denote the unitary transformation $U_{m,n} = X^m Z^n$, where $m, n = 0, 1$, and the relation (76) can be rewritten as

$$|\psi\rangle_A|\Psi^+\rangle_{BC} = \frac{1}{2}\sum_{m,n}(I\otimes U_{m,-n}\otimes U_{m,n})|\Psi^+\rangle_{AB}|\psi\rangle_C. \tag{77}$$

Here we remark that $Z^{-1} = Z$ for 2-level system. We write it in this form since this relation can be generalized directly to the general d-dimension system.

Now, suppose we do unitary transformation in the following form

$$\begin{aligned} &\sum_{\alpha,\beta} a_{\alpha,\beta}(U_{\alpha,\beta}\otimes U_{\alpha,-\beta}\otimes I)|\psi\rangle_A|\Psi^+\rangle_{BC} \\ &= \frac{1}{2}\sum_{\alpha,\beta,m,n}(U_{\alpha,\beta}\otimes U_{\alpha,-\beta}U_{m,-n}\otimes U_{m,n})|\Psi^+\rangle_{AB}|\psi\rangle_C \\ &= \sum_{m,n} b_{m,n}(I\otimes U_{m,-n}\otimes U_{m,n})|\Psi^+\rangle_{AB}|\psi\rangle_C, \end{aligned} \tag{78}$$

where we defined

$$b_{m,n} = \frac{1}{2}\sum_{\alpha,\beta}(-1)^{\alpha n-\beta m}a_{\alpha,\beta}. \tag{79}$$

The amplitudes should be normalizaed $\sum_{\alpha,\beta}|a_{\alpha,\beta}|^2 = \sum_{m,n}|b_{m,n}|^2 = 1$. This is actually the asymmetric quantum cloning machine introduced by Cerf(Cerf, 2000b). We can find the quantum states of A and C now take the form

$$\rho_A = \sum_{\alpha,\beta}|a_{\alpha,\beta}|^2 U_{\alpha,\beta}|\psi\rangle\langle\psi|U^\dagger_{\alpha,\beta}, \tag{80}$$

$$\rho_C = \sum_{m,n}|b_{m,n}|^2 U_{m,n}|\psi\rangle\langle\psi|U^\dagger_{m,n}. \tag{81}$$

The quantum state of A is related with the quantum state C by relationship between $a_{\alpha,\beta}$ and $b_{m,n}$.

The quantum state ρ_A is the original quantum state after the quantum cloning. The quantum state ρ_C is the copy.

Now, let us see a special case,

$$b_{0,0} = 1, \quad b_{0,1} = b_{1,0} = b_{1,1} = 0. \tag{82}$$

Crrespondingly, we can choose

$$a_{0,0} = a_{0,1} = a_{1,0} = a_{1,1} = \frac{1}{2}. \tag{83}$$

So, we know the quantum states of A and C have the form

$$\rho_A = \frac{1}{2}I, \quad \rho_C = |\psi\rangle\langle\psi|. \tag{84}$$

As a quantum cloning machine, this means the original quantum state in A, $|\psi\rangle$, is completely destroyed,

These results can be generalized to d-dimension system directly.

The asymmetric cloning machine was generalized to d-dimensional case by Braunstein, Bužek and Hillery(Braunstein *et al.*, 2001b). The setup is almost the same with $|\Phi^+\rangle$ instead defined in higher-dimension, $|\Phi^+\rangle = \frac{1}{\sqrt{d}}\sum_{j=1}^d |jj\rangle$, and hence the normalization relation is $a^2+b^2+2ab/d = 1$. The output reduced density matrices are written in the form with shrinking factor:

$$\rho_A = (1-b^2)|\psi\rangle\langle\psi| + b^2\frac{I}{d}, \rho_B = (1-a^2)|\psi\rangle\langle\psi| + a^2\frac{I}{d}. \tag{85}$$

Hence the fidelities are:

$$F_A = 1 - b^2\frac{d-1}{d}, F_B = 1 - a^2\frac{d-1}{d}. \tag{86}$$

If $a^2 = b^2 = d/(2d+2)$, it reduces to the symmetric 1 to 2 d-dimensional UQCM case, with fidelity $(d+3)/(2d+2)$. A trade-off relation between F_A and F_B can be found as follows (Jiang and Yu, 2010a):

$$\frac{(\sqrt{(d+1)F_A-1}+\sqrt{(d+1)F_B-1})^2}{2(d+1)} + \frac{(\sqrt{(d+1)F_A-1}-\sqrt{(d+1)F_B-1})^2}{2(d-1)} \leq 1 \tag{87}$$

Optimality is satisfied when the inequality is saturated. They also give a similar inequality for $1 \to 1+1+1$ case.

Cerf obtained the same result in a different way, here we present the d-dimensional case(Cerf, 2000a; Cerf *et al.*, 2002a). This result can be reformulated for other cases such as for state-dependent case presented in next sections. The transformation is:

$$|\psi\rangle_A \to \sum_{m,n=0}^{d-1} a_{m,n}U_{m,n}|\psi\rangle_A|B_{m,-n}\rangle_{BR} \tag{88}$$

Here $U_{m,n}$ is "generalized Pauli matrix":

$$U_{m,n} = \sum_{k=0}^{d-1} e^{\frac{2\pi kni}{d}}|k+m\rangle\langle k| \tag{89}$$

and $|B_{m,n}\rangle$ is one of the generalized Bell basis:

$$|B_{m,n}\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi kni}{d}} |k\rangle |k+m\rangle. \tag{90}$$

The resultant reduced density matrix

$$\rho_A = \sum_{m,n=0}^{d-1} |a_{m,n}|^2 U_{m,n} |\psi\rangle\langle\psi| U_{m,n}^\dagger. \tag{91}$$

Hence the fidelity $F_A = \sum_{n=0}^{d-1} |a_{0,n}|^2$. For B, we replace $a_{m,n}$ by its Fourier transform $b_{m,n} = \frac{1}{d}\sum_{m',n'=0}^{d-1} e^{2\pi(nm'-mn')i/d} a_{m',n'}$.

To clone all states equally well, the matrix a can be written in the following form:

$$a = \begin{pmatrix} v & x & \cdots & x \\ x & y & \cdots & y \\ \vdots & \vdots & \ddots & \vdots \\ x & y & \cdots & y \end{pmatrix} \tag{92}$$

with normalization relation $v^2 + 2(d-1)x^2 + (d-1)^2 y^2 = 1$. In this form, $F_A = v^2 + (d-1)x^2$ and the expression of $b_{m,n}$ is just to replace x by $x' = [v+(d-2)x+(1-d)y]/d$, y by $y' = (v-2x+y)/d$, v by $v' = [v+2(d-1)x+(d-1)^2 y]/d$. Optimal cloning requires $y = 0$, and if we let $a = v - x, b = dx$, these coincide with the parameters a and b in the first formalism. When $v = v' = \sqrt{2/(d+1)}, x = x' = \sqrt{1/(2d+2)}$, it reduces to the symmetric case. These results generalized the qutrit cloning presented by Durt and Gisin (Cerf *et al.*, 2002b).

The optimality of these cloning machines were also proved by Iblisdir *et al.*(Iblisdir *et al.*, 2005a), Fiurášek, Filip and Cerf (Fiurášek *et al.*, 2005)and Iblisdir, Acín and Gisin(Iblisdir *et al.*, 2005b). They also generalize the 1 to 2 asymmetric cloning machine to more general cases. Here we use $N \to M_1 + \cdots + M_p$ to denote such a problem: construct an asymmetric cloning machine resulting fidelity F_1 for M_1 copies, F_2 for M_2 copies, …, F_p for M_p copies.

The $1 \to 1+1+1$ d-dimensional cloning machine was constructed as following:

$$\begin{aligned} |\psi\rangle \to & \sqrt{\frac{d}{2d+2}} [\alpha|\psi\rangle_A (|\Phi^+\rangle_{BR}|\Phi^+\rangle_{CS} + |\Phi^+\rangle_{BS}|\Phi^+\rangle_{CR}) + \beta|\psi\rangle_B (|\Phi^+\rangle_{AR}|\Phi^+\rangle_{CS} + |\Phi^+\rangle_{AS}|\Phi^+\rangle_{CR}) + \\ & \gamma|\psi\rangle_C (|\Phi^+\rangle_{AR}|\Phi^+\rangle_{BS} + |\Phi^+\rangle_{AS}|\Phi^+\rangle_{BR})] \end{aligned} \tag{93}$$

where A, B, C are three output states and R, S are ancillary states. $|\Phi^+\rangle = 1/\sqrt{d}\sum_{k=0}^{d-1}|kk\rangle$ as usual. For normalization purpose, α, β, γ obey $\alpha^2 + \beta^2 + \gamma^2 + \frac{2}{d}(\alpha\beta + \beta\gamma + \alpha\gamma) = 1$. The final one copy fidelities for A, B, C are:

$$\begin{aligned} F_A &= 1 - \frac{d-1}{d}\left(\beta^2 + \gamma^2 + \frac{2\beta\gamma}{d+1}\right) \\ F_B &= 1 - \frac{d-1}{d}\left(\alpha^2 + \gamma^2 + \frac{2\alpha\gamma}{d+1}\right) \\ F_C &= 1 - \frac{d-1}{d}\left(\alpha^2 + \beta^2 + \frac{2\alpha\beta}{d+1}\right). \end{aligned} \tag{94}$$

In (Iblisdir *et al.*, 2005a), the $1 \to 1+n$ cloning machine was found. The Hilbert space $\mathcal{H}^{\otimes(n+1)}$ is decomposed into two symmetric subspace $\mathcal{H}^+_{n+1} \oplus \mathcal{H}^+_{n-1}$. Let s_{n+1} and s_{n-1} denote the projection operator, respectively, the transformation can be written as:

$$T : \rho \to (\alpha^* s_{n+1} + \beta^* s_{n-1})(\rho \otimes I^{\otimes n})(\alpha s_{n+1} + \beta s_{n-1}). \tag{95}$$

It is a generalization of the construction of symmetric UQCM (57). The resulting fidelity is $F_A = 1 - \frac{2}{3}y^2$ for the '1' side, and $F_B = \frac{1}{2} + \frac{1}{3n}(y^2 + \sqrt{n(n+2)}xy)$. Here x and y satisfy $x^2 + y^2 = 1$. A more general case, $N \to M_A + M_B$, is studied with similar method in (Iblisdir *et al.*, 2005b).

In studying asymmetric quantum cloning, the region of possible output fidelities for one to three cloning is studied in (Jiang and Yu, 2010a), the case of one to many case is studied in (Cwiklinski *et al.*, 2012), the general case is studied in (Kay *et al.*, 2012).

D. A unified UQCM

Recently, Wang *et al.* proposed a unified way to construct general asymmetric UQCM (Wang *et al.*, 2011b). The essence is to replace the symmetric operator s_M in construction (69) by a linear combination of identity I and many permutation operators. Take the 1 to 2 qubit cloning case as the simplest example, $s_2 = \frac{1}{2}(I^{\otimes 2} + \mathcal{P})$, where $\mathcal{P} = |00\rangle\langle 00| + |11\rangle\langle 11| + |01\rangle\langle 10| + |10\rangle\langle 01|$ is a permutation(swap) operator($\mathcal{P}|jl\rangle = |lj\rangle$). If s_2 is replaced by $\alpha I^{\otimes 2} + \beta\mathcal{P}$, the output density matrix exactly coincides with the output density matrix in construction (72): $|\psi\rangle_A \to a|\psi\rangle_A|\Phi^+\rangle_{BR} + b|\psi\rangle_B|\Phi^+\rangle_{AR}$, with $\alpha = \frac{\sqrt{3}}{2}a, \beta = \frac{\sqrt{3}}{2}b$.

In order to introduce this method, here we present two examples to show explicitly that it can be applied straightforwardly for various occasions.

For $1 \to 3$ asymmetric qubit cloning case, we replace the symmetry operator s_3 by

$$\alpha I + \beta\mathcal{P}_{12} + \gamma\mathcal{P}_{13} + \delta\mathcal{P}_{23} + \mu\mathcal{P}_{123} + \nu\mathcal{P}_{132}. \tag{96}$$

Note $\mathcal{P}_{mn}$ is the operator that swap the m qubit and the n qubit, and $\mathcal{P}_{123}$ is a cyclic operator that move the first qubit to the second place, the second qubit to the third place, and the third qubit to the first place. $\mathcal{P}_{132}$ is its inverse transformation. In fact these six components in (96) are just the elements of permutation group S_3. The symmetry operator $s_3 = \frac{1}{6}(I + \mathcal{P}_{12} + \mathcal{P}_{13} + \mathcal{P}_{23} + \mathcal{P}_{123} + \mathcal{P}_{132})$, is retrieved when $\alpha = \beta = \gamma = \delta = \mu = \nu = \frac{1}{6}$. The $1 \to 3$ asymmetric qubit cloning can be obtained by replacing s_3 by (96) and insert it to the cloning transformation (69). Here we would like to remark that the number of essential permutations for the specific $1 \to 3$ case are actually three. There are only three independent parameters corresponding to cases: the input state is in first, second, and third positions, respectively. This will be shown explicitly later. Now, if we trace out the ancillary states, it is equivalent to modify (57). The final density operator is:

$$\begin{aligned}
\rho &= \frac{1}{2}(\alpha I + \beta\mathcal{P}_{12} + \gamma\mathcal{P}_{13} + \delta\mathcal{P}_{23} + \mu\mathcal{P}_{123} + \nu\mathcal{P}_{132})(|\psi\rangle\langle\psi| \otimes I \otimes I)(\alpha I + \beta\mathcal{P}_{12} + \gamma\mathcal{P}_{13} + \delta\mathcal{P}_{23} + \mu\mathcal{P}_{123} + \nu\mathcal{P}_{132})\\
&= \frac{1}{2}[\alpha|\psi\rangle\langle\psi| \otimes I \otimes I + \beta(|0\psi\rangle\langle\psi 0| + |1\psi\rangle\langle\psi 1|) \otimes I_3 + \gamma(|0\psi\rangle\langle\psi 0| + |1\psi\rangle\langle\psi 1|)_{13} \otimes I_2\\
&+ \delta|\psi\rangle\langle\psi|_1 \otimes (|00\rangle\langle 00| + |11\rangle\langle 11| + |01\rangle\langle 10| + |10\rangle\langle 01|) + \mu(|0\psi 0\rangle\langle\psi 00| + |1\psi 0\rangle\langle\psi 01| + |0\psi 1\rangle\langle\psi 10| + |1\psi 1\rangle\langle\psi 11|)\\
&+ \nu(|00\psi\rangle\langle\psi 00| + |01\psi\rangle\langle\psi 01| + |10\psi\rangle\langle\psi 10| + |11\psi\rangle\langle\psi 11|)](\alpha I + \beta\mathcal{P}_{12} + \gamma\mathcal{P}_{13} + \delta\mathcal{P}_{23} + \mu\mathcal{P}_{123} + \nu\mathcal{P}_{132})\\
&= \frac{1}{2}[(\alpha^2 + \delta^2)|\psi\rangle\langle\psi| \otimes I \otimes I + (\beta^2 + \mu^2)I \otimes |\psi\rangle\langle\psi| \otimes I + (\gamma^2 + \nu^2)I \otimes I \otimes |\psi\rangle\langle\psi|\\
&+ (\alpha\beta + \mu\delta)(|\psi 0\rangle\langle 0\psi| + |\psi 1\rangle\langle 1\psi| + |0\psi\rangle\langle\psi 0| + |1\psi\rangle\langle\psi 1|)_{12} \otimes I_3\\
&+ (\alpha\gamma + \nu\delta)(|\psi 0\rangle\langle 0\psi| + |\psi 1\rangle\langle 1\psi| + |0\psi\rangle\langle\psi 0| + |1\psi\rangle\langle\psi 1|)_{13} \otimes I_2\\
&+ (\beta\gamma + \mu\nu)(|00\psi\rangle\langle 0\psi 0| + |01\psi\rangle\langle 1\psi 0| + |10\psi\rangle\langle 0\psi 1| + |11\psi\rangle\langle 1\psi 1| + trans.)\\
&+ (\delta\beta + \alpha\mu)(|0\psi 0\rangle\psi 00| + |0\psi 1\rangle\psi 10| + |1\psi 0\rangle\langle\psi 01| + |1\psi 1\rangle\langle\psi 11| + trans.)\\
&+ \delta\gamma(|0\psi 0\rangle\langle 00\psi| + |0\psi 1\rangle\langle 10\psi| + |1\psi 0\rangle\langle 01\psi| + |1\psi 1|\rangle\langle 11\psi| + trans.)\\
&+ (\beta\nu + \gamma\mu)I_1 \otimes (|\psi 0\rangle\langle 0\psi| + |\psi 1\rangle\langle 1\psi| + |0\psi\rangle\langle\psi 0| + |1\psi\rangle\langle\psi 1|)_{23}\\
&+ \alpha\nu(|00\psi\rangle\langle\psi 00| + |01\psi\rangle\langle\psi 01| + |10\psi\rangle\langle\psi 10| + |11\psi\rangle\psi 11| + trans.)\\
&+ 2\alpha\delta|\psi\rangle\langle\psi|_1 \otimes (|00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|)_{23}\\
&+ 2\beta\mu|\psi\rangle\langle\psi|_2 \otimes (|00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|)_{13}\\
&+ 2\gamma\nu|\psi\rangle\langle\psi|_3 \otimes (|00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|)_{12}
\end{aligned} \tag{97}$$

Here *trans.* denotes the rotation of previous terms. Trace out the second and third qubits, we obtain the single qubit reduced density matrix,

$$\begin{aligned}
\rho_1 &= [2(\alpha^2 + \delta^2 + \alpha\delta) + \alpha(2\beta + 2\gamma + \mu + \nu) + \delta(2\mu + 2\nu + \beta + \gamma) + \mu\nu + \beta\gamma]|\psi\rangle\langle\psi|\\
&+ (\beta^2 + \mu^2 + \gamma^2 + \nu^2 + \beta\mu + \beta\nu + \gamma\mu + \gamma\nu)I
\end{aligned} \tag{98}$$

Hence a normalization relation is easily obtained:

$$\begin{aligned}
&2(\alpha^2 + \delta^2 + \alpha\delta) + \alpha(2\beta + 2\gamma + \mu + \nu) + \delta(2\mu + 2\nu + \beta + \gamma) + \mu\nu + \beta\gamma +\\
&2(\beta^2 + \mu^2 + \gamma^2 + \nu^2 + \beta\mu + \beta\nu + \gamma\mu + \gamma\nu) = 1
\end{aligned} \tag{99}$$

Similarly we can find the reduced density matrices of the second and third copies, their fidelities are:

$$\begin{aligned}F_1 &= 1-\frac{1}{2}[(\beta+\mu)^2+(\beta+\nu)^2+(\gamma+\mu)^2+(\gamma+\nu)^2]\\ F_2 &= 1-\frac{1}{2}[(\alpha+\delta)^2+(\alpha+\nu)^2+(\gamma+\delta)^2+(\gamma+\nu)^2]\\ F_3 &= 1-\frac{1}{2}[(\alpha+\delta)^2+(\alpha+\mu)^2+(\beta+\delta)^2+(\beta+\mu)^2]\end{aligned}\tag{100}$$

It reduces to the symmetric cloning case when $\alpha=\beta=\gamma=\delta=\mu=\nu=\frac{1}{6}$, and the fidelity is 7/9, which exactly coincide with the UQCM fidelity formula (59). To see its relation with the previous $1\to 3$ asymmetric UQCM (93), we can explicitly compute out the density matrix in (93):

$$\begin{aligned}\rho_{out} = \frac{1}{12}\{&4(\alpha'|\psi00\rangle+\beta'|0\psi0\rangle+\gamma'|00\psi\rangle)(\alpha'\langle\psi00|+\beta'\langle0\psi0|+\gamma'\langle00\psi|)\\ &+2[\alpha'(|\psi01\rangle+\psi10\rangle)+\beta'(|0\psi1\rangle+|1\psi0\rangle)+\gamma'(|01\psi\rangle+|10\psi\rangle)]\\ &[\alpha'(\langle\psi01|+\langle\psi10|)+\beta'(\langle0\psi1|+\langle1\psi0|)+\gamma'(\langle01\psi|+\langle10\psi|)]\\ &+4(\alpha'|\psi11\rangle+\beta'|1\psi1\rangle+\gamma'|11\psi\rangle)(\alpha'\langle\psi11|+\beta'\langle1\psi1|+\gamma'\langle11\psi|)\}\end{aligned}\tag{101}$$

For clarity purpose we replace the coefficients α,β,γ in (93) with α',β',γ'. Compare this expression with (97), we found if the following equations are satisfied, they are equivalent:

$$\begin{aligned}&\frac{\alpha'^2}{3}=(\alpha+\delta)^2,\frac{\beta'^2}{3}=(\beta+\mu)^2,\frac{\gamma'^2}{3}=(\gamma+\nu)^2\\ &\alpha'^2=12\alpha\delta,\beta'^2=12\beta\mu,\gamma'^2=12\gamma\nu.\end{aligned}\tag{102}$$

This implies $\alpha=\delta=\alpha'/(2\sqrt{3}),\beta=\mu=\beta'/(2\sqrt{3}),\gamma=\nu=\gamma'/(2\sqrt{3})$. And in this case the fidelity expressions (100) exactly coincide with the previous results (94). The cloning machine here has six parameters, which indicates that it is a general form of asymmetric UQCM, and we do not need to consider the specific input positions.

We can study the $2\to 3$ case similarly. The resultant density matrix is:

$$\begin{aligned}\rho &= \frac{1}{2}(\alpha I+\beta\mathcal{P}_{12}+\gamma\mathcal{P}_{13}+\delta\mathcal{P}_{23}+\mu\mathcal{P}_{123}+\nu\mathcal{P}_{132})(|\psi\psi\rangle\langle\psi\psi|\otimes I)(\alpha I+\beta\mathcal{P}_{12}+\gamma\mathcal{P}_{13}+\delta\mathcal{P}_{23}+\mu\mathcal{P}_{123}+\nu\mathcal{P}_{132})\\ &= \frac{1}{2}[(\alpha+\beta)|\psi\psi\rangle\langle\psi\psi|\otimes I_3+(\gamma+\mu)(|0\psi\psi\rangle\langle\psi\psi0|+|1\psi\psi\rangle\langle\psi\psi1|)\\ &+(\delta+\nu)(|\psi0\psi\rangle\langle\psi\psi0|+|\psi1\psi\rangle\langle\psi\psi1|)](\alpha I+\beta\mathcal{P}_{12}+\gamma\mathcal{P}_{13}+\delta\mathcal{P}_{23}+\mu\mathcal{P}_{123}+\nu\mathcal{P}_{132})\\ &= \frac{1}{2}[(\alpha+\beta)^2|\psi\psi\rangle\langle\psi\psi|\otimes I_3+(\gamma+\mu)^2I_1\otimes|\psi\psi\rangle\langle\psi\psi|+(\delta+\nu)^2|\psi\rangle\langle\psi|\otimes I_2\otimes|\psi\rangle\langle\psi|\\ &+(\alpha+\beta)(\gamma+\mu)(|0\psi\psi\rangle\langle\psi\psi0|+|1\psi\psi\rangle\langle\psi\psi1|+trans.)\\ &+(\alpha+\beta)(\delta+\nu)(|\psi0\psi\rangle\langle\psi\psi0|+|\psi1\psi\rangle\langle\psi\psi1|+trans.)\\ &+(\gamma+\mu)(\delta+\nu)(|\psi0\psi\rangle\langle0\psi\psi|+|\psi1\psi\rangle\langle1\psi\psi|+trans.)\end{aligned}\tag{103}$$

We can see that there are only three independent parameters in the final expression: $\alpha+\beta$, $\gamma+\mu$, $\delta+\nu$, so we denote them by A, B and C respectively. We trace out the other two states to obtain the following one copy reduced density matrices:

$$\begin{aligned}\rho_1 &= (A^2+C^2+AB+AC+BC)|\psi\rangle\langle\psi|+\frac{B^2}{2}I\\ \rho_2 &= (A^2+B^2+AB+AC+BC)|\psi\rangle\langle\psi|+\frac{C^2}{2}I\\ \rho_3 &= (B^2+C^2+AB+AC+BC)|\psi\rangle\langle\psi|+\frac{A^2}{2}I\end{aligned}\tag{104}$$

The coefficients apparently satisfy a normalization relation: $A^2+B^2+C^2+AB+BC+CA=1$. From the one copy reduced density matrices we simply read out the fidelities:

$$F_1=1-\frac{B^2}{2},F_2=1-\frac{C^2}{2},F_3=1-\frac{A^2}{2}\tag{105}$$

For symmetric cloning case, we let $A=B=C=1/\sqrt{6}$, then the fidelity is 11/12, which exactly coincide with the UQCM fidelity formula (59).

E. Singlet monogamy and optimal cloning

In quantum information science, entanglement is a resource for various QIP applications. On the other hand, the entanglement cannot be shared freely among multi-parties. For example, for a multipartite quantum state, one party cannot be maximally entangled independently with other two parties simultaneously. It means that entanglement is monogamous. There are some monogamy inequalities for entanglement sharing (Coffman *et al.*, 2000; Osborne and Verstraete, 2006; Ou and Fan, 2007; Ou *et al.*, 2008).

In this review, we consider the singlet monogamy in application of quantum cloning. We know that singlet is a natural maximally entangled state, we use the name of singlet monogamy to describe the restrictions on entanglement sharing.

Quantitatively, the amount of entanglement between A and B can be defined as

$$p_{A,B} = \max_{U,V} \langle \Phi^+ | U \otimes V \rho_{A,B} U^\dagger \otimes V^\dagger | \Phi^+ \rangle \tag{106}$$

where $|\Phi^+\rangle = \sum_{i=0}^{d-1} |ii\rangle/\sqrt{d}$ is the d-dimensional maximally entangled state, which is standard in this review. This quantity describes, under local unitary operations, the fidelity between state $\rho_{A,B}$ and the maximally entangled state. In (Kay *et al.*, 2009), Kay, Kaszlikowski and Ramanathan discovered the relation between singlet monogamy and $1 \to N$ optimal asymmetric UQCM. In their approach, a setup proposed by Fiurášek(Fiurášek, 2001a) is used: $\Lambda_{out}(\psi_{in})$ is a reduced density matrix so that the efficiency of this cloning machine F is measured by averaging $Tr[\sqrt{\sqrt{\rho_{in}}\Lambda_{out}(\psi_{in})\sqrt{\rho_{in}}}]^2$. Note this is a "average" definition of fidelity. In (Fiurášek, 2001a) it is proved $F \leq d\lambda$ where λ is the maximal eigenvalue of the matrix

$$R = \int \mathrm{d}\psi_{in} [|\psi_{in}\rangle\langle\psi_{in}|^T \otimes \Lambda_{out}(\psi_{in})]. \tag{107}$$

For the specific $1 \to N$ asymmetric cloning case, $\Lambda_{out}(\psi_{in})$ is defined to be

$$\Lambda_{out}(\psi_{in}) = \sum_{i=1}^{N} \alpha_i I_1 \otimes \cdots \otimes I_{i-1} \otimes |\psi_{in}\rangle\langle\psi_{in}|_i \otimes I_{i+1} \otimes \cdots \otimes I_N. \tag{108}$$

Here α_i is a set of parameters to describe the required asymmetry of output states, which satisfies $\sum_{i=1}^N \alpha_i = 1$. Rewriting $|\psi_{in}\rangle$ as $U|0\rangle$, where U is a unitary operator in d-dimensional Hilbert space, then from (107) we find

$$R = \int \mathrm{d}U \sum_{i=1}^{N} \alpha_i U^T \otimes U |00\rangle\langle 00|_{0,i} U^* \otimes U^\dagger, \tag{109}$$

where the subscript 0 denotes a state entangled with the N output states, which just comes from $|\psi_{in}\rangle\langle\psi_{in}|^T$ in expression (107). After calculation it turns out to be

$$R = \frac{1}{d(d+1)} \sum_{i=1}^{N} \alpha_i |\Phi^+\rangle\langle\Phi^+|_{0,i}. \tag{110}$$

To find out the eigenvalue of this matrix, an ansatz is proposed:

$$|\Psi\rangle = \sum_{i=1}^{N} \beta_i |\Phi^+\rangle|\Phi\rangle_{1\ldots(i-1)(i+1)\ldots N}. \tag{111}$$

β_i is parameters satisfy normalization condition $(\sum_{i=1}^N \beta_i)^2 + (d-1)\sum_{i=1}^N \beta_i^2 = d$, and $|\Phi\rangle$ means a normalized superposition of all permutation of $|\Phi^+\rangle^{\otimes(N-1)/2}$ for odd N and $|\Phi^+\rangle^{\otimes(N-2)/2}|0\rangle$ for even N. It satisfies

$$(|\Phi^+\rangle\langle\Phi^+|_{0,j} \otimes I)|\Phi\rangle_{0,i}|\Phi\rangle_{1\ldots(i-1)(i+1)\ldots N} = \gamma_{i,j}|\Phi^+\rangle_{0,j}|\Phi\rangle_{1\ldots(j-1)(j+1)\ldots N}. \tag{112}$$

Here $\gamma_{i,j} = [1 + \delta_{ij}(d-1)]/d$ and hence we know $|\Psi\rangle$ is a eigenvector of R if $\alpha_i d \sum_{j=1}^N \gamma_{i,j}\beta_j = [d(d+1) - \lambda]\beta_i$ for every i. Combine this constraint with the expression of singlet monogamy of $|\Psi\rangle$: $p_{0,i} = (\sum_{j=1}^N \gamma_{i,j}\beta_j)^2$, as well as the normalization condition, we get the singlet monogamy relation for $1 \to N$ asymmetric cloning machine:

$$\sum_{i=1}^{N} p_{0,i} \leq \frac{d-1}{d} + \frac{1}{N+d-1}(\sum_{i=1}^{N} \sqrt{p_{0,i}})^2. \tag{113}$$

It is straightforward to find the one copy fidelity $F_i = (p_{0,i}d + 1)/(d + 1)$. For symmetric UQCM case, one let all $p_{0,i}$ to be equal to $(N + d - 1)/dN$ and then the previous result $F = (2N + d - 1)/[N(d + 1)]$ is regenerated. In (Kay *et al.*, 2009) it is also shown that the previous $1 \to 1 + 1 + 1$ asymmetric cloning and $1 \to 1 + N$ asymmetric cloning cases are consistent with this approach.

The $1 \to 4$ asymmetric cloning can be similarly studied (Ren *et al.*, 2011). The normalization condition in this specific case turns out to be:

$$\beta_1^2 + \beta_2^2 + \beta_3^2 + \beta_4^2 + \frac{2}{d}(\beta_1\beta_2 + \beta_1\beta_3 + \beta_1\beta_4 + \beta_2\beta_3 + \beta_2\beta_4 + \beta_3\beta_4) = 1 \tag{114}$$

and the fidelity of these four copies are:

$$F_1 = 1 - \frac{d-1}{d}[\beta_2^2 + \beta_3^2 + \beta_4^2 + \frac{2(\beta_2\beta_3 + \beta_2\beta_4 + \beta_3\beta_4)}{d+1}], \tag{115}$$

$$F_2 = 1 - \frac{d-1}{d}[\beta_1^2 + \beta_3^2 + \beta_4^2 + \frac{2(\beta_1\beta_3 + \beta_1\beta_4 + \beta_3\beta_4)}{d+1}], \tag{116}$$

$$F_3 = 1 - \frac{d-1}{d}[\beta_1^2 + \beta_2^2 + \beta_4^2 + \frac{2(\beta_1\beta_2 + \beta_1\beta_4 + \beta_2\beta_4)}{d+1}], \tag{117}$$

$$F_4 = 1 - \frac{d-1}{d}[\beta_1^2 + \beta_2^2 + \beta_3^2 + \frac{2(\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3)}{d+1}]. \tag{118}$$

With general asymmetric quantum cloning machine available, we can expect that the corresponding relationship between quantum cloning and entanglement monogamy can be constructed.

F. Mixed-state quantum cloning

In the previous discussions of quantum cloning, the input state is assumed to be pure. What if the input state is mixed state ρ? Sometimes since we only look at the resulted local one-copy reduced density matrix, this procedure is named "broadcasting"(Barnum *et al.*, 1996; D'Ariano *et al.*, 2005b), as we already presented in this review. In (Barnum *et al.*, 1996), Barnum *et al.* proved the $1 \to 2$ no cloning theorem can be extended to mixed state case, that is, for two non-commuting input density matrices, the cloning machine cannot copy both perfectly, as we have already shown in previous sections. Then D'Ariano, Macchiavello and Perinotti studied the extended $N \to M$ case and constructed the optimal UQCM (D'Ariano *et al.*, 2005b). They found a non-trivial result that the no-broadcasting theorem cannot be generalized to more than one input case. Specifically, for UQCM, it is even possible to purify the input states when $N \geq 4$, this phenomenon is called "superbroadcasting". Note here UQCM does not mean constant fidelity reached for every mixed state, since the existence of such cloning machine ($1 \to M$) was nullified by Chen and Chen (Chen and Chen, 2007b). For mixed state cloning, it seems reasonable to use the shrinking factor as the measure of merit for the quantum cloning machine. This is for cloning of mixed states in symmetric subspace (Fan, 2003). The property of "universal" for mixed cloning machine is in the sense that the shrinking factor of the single output is independent of the input mixed state.

In this subsection, we try to review some explicit results of mixed state cloning studied in (Dang and Fan, 2007; Fan *et al.*, 2007; Yang *et al.*, 2007). The UQCM for pure state (57,64) can be applied apparently to one input mixed state. But if we input the direct product of two identical ρ, direct application of (57) cannot give the optimal output. This can be easily figured out if we consider the $2 \to 2$ case. The optimal transformation is just leaving it unchanged, but if we apply the symmetrization projection, since $\rho \otimes \rho$ contains an asymmetric part, this part is deleted so the final state changes. So we need to find out other ways to achieve maximal fidelity.

We suppose the input state is identical copies of $\rho = z_0|0\rangle\langle 0| + z_1|0\rangle\langle 1| + z_2|1\rangle\langle 0| + z_3|1\rangle\langle 1|$, and we use the notation $|m, n\rangle$ to denote the totally symmetric state with m $|0\rangle$s and n $|1\rangle$s. Additionally we introduce $|\widetilde{m,n}\rangle$ which is constructed by multiplying each components in $|m, n\rangle$ by a number of $\omega = \exp[2\pi i m!n!/(m + n)!]$. For example, $|\widetilde{2,1}\rangle = (|001\rangle + \omega|010\rangle + |100\rangle)/\sqrt{3}$. Obviously $|m, n\rangle$ is orthogonal to $|\widetilde{m,n}\rangle$.

Then the $2 \to 3$ transformation is written as:

$$\begin{aligned}
|2,0\rangle|R\rangle &\to \sqrt{\frac{3}{4}}|3,0\rangle|R_0\rangle + \sqrt{\frac{1}{4}}|2,1\rangle|R_1\rangle \\
|1,1\rangle|R\rangle &\to \sqrt{\frac{1}{2}}|2,1\rangle|R_0\rangle + \sqrt{\frac{1}{2}}|1,2\rangle|R_1\rangle \\
|0,2\rangle|R\rangle &\to \sqrt{\frac{1}{4}}|1,2\rangle|R_0\rangle + \sqrt{\frac{3}{4}}|0,3\rangle|R_1\rangle \\
|\widetilde{1,1}\rangle|R\rangle &\to \sqrt{\frac{1}{2}}|\widetilde{2,1}\rangle|R_0\rangle + \sqrt{\frac{1}{2}}|\widetilde{1,2}\rangle|R_1\rangle.
\end{aligned} \tag{119}$$

It can be verified that the output single copy reduced density matrix is $\frac{5}{6}\rho + \frac{I}{12}$. The shrinking factor $5/6$, apparently coincide with the maximal shrinking factor of $2 \to 3$ UQCM in pure state case. The more general $2 \to M$ mixed state cloner is constructed in similar way:

$$\begin{aligned}
|2,0\rangle|R\rangle &\to \sum_{k=0}^{M-2} \alpha_{0k}|M-k,k\rangle|R_k\rangle \\
|1,1\rangle|R\rangle &\to \sum_{k=0}^{M-2} \alpha_{1k}|M-k-1,k+1\rangle|R_k\rangle \\
|0,2\rangle|R\rangle &\to \sum_{k=0}^{M-2} \alpha_{2k}|M-k-2,k+2\rangle|R_k\rangle \\
|\widetilde{1,1}\rangle|R\rangle &\to \sum_{k=0}^{M-2} \alpha_{1k}|M-\widetilde{k-1,k}+1\rangle|R_k\rangle
\end{aligned} \tag{120}$$

where

$$\alpha_{jk} = \sqrt{\frac{6(M-2)!(M-j-k)!(j+k)!}{(2-j)!(M+1)!(M-2-k)!j!k!}}. \tag{121}$$

By calculations, it can also be shown that the shrinking factor leads to previous results(59) corresponding for pure state case, hence it's optimal.

In (Dang and Fan, 2007) this construction is generalized to $N \to M$ case:

$$|N-m,m\rangle|R\rangle \to \sum_{k=0}^{M-N} \beta_{mk}|M-m-k,m+k\rangle|R_{M-N-k,k}\rangle, \tag{122}$$

the coefficients are:

$$\beta_{mk} = \sqrt{\frac{(M-N)!\,(N+1)!}{(M+1)!}}\sqrt{\frac{(M-m-k)!}{(N-m)!\,(M-N-k)!}} \cdot \sqrt{\frac{(m+k)!}{m!k!}}. \tag{123}$$

G. Universal NOT gate

Similar to the quantum cloning problem, one can ask if there is some transformation U that convert an arbitrary state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to its conjugate state $|\psi^\perp\rangle = \beta^*|0\rangle - \alpha^*|1\rangle$. For two states $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\psi_2\rangle = \gamma|0\rangle + \delta|1\rangle$, we have $\langle\psi_2|\psi_1\rangle = \gamma^*\alpha + \delta^*\beta = \big(\langle\psi_2|U^\dagger U|\psi_1\rangle\big)^*$, hence U is an anti-unitary operator. And it is not completely positive hence cannot be applied to a small system, as argued by Bužek, Hillery and Werner in (Bužek *et al.*, 1999).

Then it is a question whether we can have a universal NOT gate approximately. A general $N \to M$ universal NOT gate is constructed by using the universal cloning machine. The final single copy output density matrix is $\rho_{out,1} = \frac{N}{N+2}|\psi^\perp\rangle\langle\psi^\perp| + \frac{1}{N+2}I$, regardless of M. In fact, this is exactly the reduced density matrix of the ancilla in the UQCM. This is an interesting result since it shows the ancilla has the “anti-clone” meaning. The optimality of this universal NOT gate is also proved (Bužek and Hillery, 2000). The universal NOT gate or anti-cloning is the same

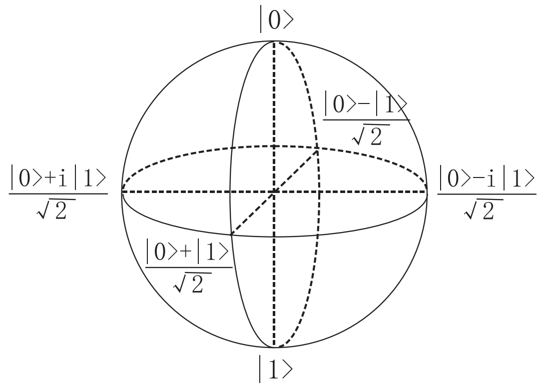


FIG. 2 The six states used in quantum key distribution, the optimal cloning machine to clone those six states is a UQCM.

as the universal spin flip machine (Gisin and Popescu, 1999). Related, it is found that a pair of antiparallel spins can contain more information than that of parallel spins. The universal NOT gate is studied for continuous variable system in (Cerf and Iblisdir, 2001a). The experimental implementation of universal NOT gate in optical system is reported in (De Martini *et al.*, 2002).

H. Minimal input set, six-state cryptography and other results

Bruss showed that the $1 \to 2$ optimal cloning of the following six states with equal fidelity for each state is equivalent to the qubit UQCM(Bruß, 1998),

$$\begin{aligned}&\{|0\rangle, |1\rangle\};\\&\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\};\\&\{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}.\end{aligned} \tag{124}$$

These six states can be represented on Bloch sphere as FIG.2.

These six states are exactly the three basis used in the six-state QKD protocol, and indeed the UQCM can be regarded as the optimal way to attack the quantum channel in this protocol (Bechmann-Pasquinucci and Gisin, 1999). This is an interesting phenomenon, it means that the optimal cloning machine for those six states can actually clone arbitrary qubits optimally. On the other hand, it also means that we cannot clone six states better than a UQCM does.

A reverse question might be interesting: how many states are enough to define a UQCM? More explicitly, what is the minimal number of the states in the input set, such that the optimal cloning machine that achieves equal fidelity for them is equivalent to the UQCM? Jing *et al.* (Jing *et al.*, 2012) solved this problem in the $1 \to 2$ cloning case. The minimal set turns out to be four states on the vertex of a tetrahedron:

$$\begin{aligned}|\psi_1\rangle &= |0\rangle,\\|\psi_2\rangle &= \cos(\theta/2)|0\rangle + \sin(\theta/2)|1\rangle,\\|\psi_3\rangle &= \cos(\theta/2)|0\rangle + \sin(\theta/2)e^{2i\pi/3}|1\rangle,\\|\psi_4\rangle &= \cos(\theta/2)|0\rangle + \sin(\theta/2)e^{4i\pi/3}|1\rangle,\end{aligned} \tag{125}$$

where θ satisfies $\cos(\theta/2) = \frac{\sqrt{3}}{3}$, see FIG.3.

There is a similar phenomenon for states on the equator of the Bloch sphere, which will be demonstrated in the following section.

I. Other developments and related topics

Other works related with universal cloning include: Gisin and Huttner pointed out the relationships between quantum cloning, eavesdropping of quantum key distributions and the Bell inequalities (Gisin and Huttner, 1997). Jiang

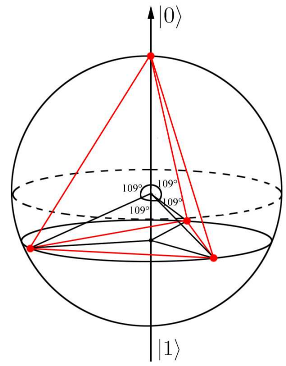


FIG. 3 The four states on the vertex of a tetrahedron, which determines a UQCM in $1 \to 2$ cloning case.

and Yu constructed a Hamiltonian realization of UQCM, and the maximal eigenvalue of this Hamiltonian matrix is the fidelity (Jiang and Yu, 2010b). The spin networks is also possible to realize the UQCM (De Chiara *et al.*, 2004). Pang, Wu and Chen proved the non-existence of a universal quantum machine to examine the precision of unknown quantum states, which is related to UQCM (Pang *et al.*, 2011). Roubert and Braun studied the introduction of interference in UQCM and found that it does not affect the 5/6 optimal 1 to 2 qubit symmetric cloning result (Roubert and Braun, 2008). If the ancillary state is not ideally initialed, its effect on the optimal UQCM is studied in (Zhang *et al.*, 2012). The one to many universal cloning machine was studied in (Albeverio and Fei, 2000). Mixed state cloning is also related with cloning of states with temperature effects (Baghbanzadeh and Rezakhani, 2009). The cloning is related with optimizing the completely maps using semidefinite programming (Audenaert and De Moor, 2002). The measurements on various subsystems of the cloning machine is studied in (Bruß *et al.*, 2001). Asymptotically, the quantum cloning machine corresponds to state estimation (Bae and Acín, 2006; Bruß *et al.*, 1998b; Derka *et al.*, 1998), for d-dimensional case see (Bruß and Macchiavello, 1999). Also there exists a tradeoff relation between the information gain and the disturbance on the estimated state (Banaszek, 2001), also in (Maccone, 2006) and (Kretschmann *et al.*, 2008), this should be related with the asymmetric quantum cloning. The same type of trade-off relations between measurement accuracy of two or three non-commuting observables of a qubit system is studied in (Sagawa and Ueda, 2008), this leads to the no-cloning inequality. The application of this method in quantum communication and the separability of quantum and classical information is studied in (Ricci *et al.*, 2005). The realization of UQCM is proposed in optical system (Filip, 2004a,b; Irvine *et al.*, 2004). The asymmetric UQCM is realized experimentally by partial teleportation (Zhao *et al.*, 2005). The asymmetric quantum cloning machine is realized experimentally by polarization states of single photons (Cernoch *et al.*, 2009). The experimental quantum cloning can also be realized by using photons orbital angular momentum (Nagali *et al.*, 2009). If both polarization and orbital angular momentum degrees of freedom of photons are used, the four-dimensional quantum state can be encoded. The experimental cloning of four-dimension state by this scheme is demonstrated in (Nagali *et al.*, 2010). The general UQCM realized by projective operators and stochastic maps is investigated both theoretically and experimentally presented in (Sciarrino *et al.*, 2004b). The reverse of quantum cloning is also studied in photon stimulated emission scheme (Raeisi *et al.*, 2012) and in continuous variable system (Filip *et al.*, 2004). By photon polarization in optics system, the universal quantum cloning and universal NOT gate is implemented experimentally (Sciarrino *et al.*, 2004a). A recent review about photonic quantum information processing can be found in (Martini and Sciarrino, 2012; Pan *et al.*, 2012).

It is shown that a pair of qubits with anti-parallel spins may encode more quantum information (Gisin and Popescu, 1999), collective and local measurements of them is studied in (Massar, 2000), the cloning of those kind of states is studied in (Fiurášek *et al.*, 2002). The state estimation is corresponding to one to infinity quantum cloning, and it roughly describes how to find the exact form of an unknown state. The problem of learning an unknown unitary transformation from a finite number of examples is related, but different from cloning which is studied in (Bisio *et al.*, 2010). The cloning of a quantum measurement is studied in (Bisio *et al.*, 2011). Two incompatible observables cannot be measured simultaneously for a quantum system, the cloning schemes are studied for this task to accomplish it optimally (Brougham *et al.*, 2006). As one application, the UQCM is adopted to investigate the entanglement and the quantum coherence of the output field in the high-gain quantum injected parametric amplification (Caminati *et al.*, 2006). The superbroadcasting is also applied for a method that broadcasting and simultaneous purification of the local output states are performed (Chiribella *et al.*, 2007). The upper found of global fidelity for mixed state universal cloning and state-dependent cloning are obtained in (Rastegin, 2003b) and in (Rastegin, 2003a). The optimal minimal measurements of mixed states is studied in (Vidal *et al.*, 1999). The repeatable quantum channels with quantum memory is studied in (Rybar and Ziman, 2008), this topic is closely related with quantum cloning. Several cases

of qubit quantum cloning combinations are also investigated in (Wu and Wu, 2012). The high fidelity copies from asymmetric cloning machine are studied in (Siomau and Fritzsche, 2010a). The universal controlled-NOT gate is studied in (Siomau and Fritzsche, 2010b). Numerical calculations are performed to study the relationships between fidelities of cloning machines and the entanglement (Durt and Van de Putte, 2011). Related, the optimal realization of the transposition maps is studied in (Buscemi *et al.*, 2003). In relativistical quantum information, a trade-off relation is studied for universal cloning of qudit (Jochym-O'Connor *et al.*, 2011).

The possibility to improve the fidelity of the UQCM in the photon stimulated emission scheme is studied in (Dasgupta and Agarwal, 2001). The broadband photon cloning and the entanglement creation of atoms in waveguide is studied in (Valente *et al.*, 2012). The application of cloning machine to improve the detectors is in (Deuar and Munro, 2000a). The information transfer, and the information in practical in cloning machine are presented in (Deuar and Munro, 2000b) and (Deuar and Munro, 2000c). The information flux in many body system and in quantum cloning machine is studied in (Di Franco *et al.*, 2007). The universal cloning by entangled parametric amplification is studied in (De Martini *et al.*, 2000). The proposals to implement cloning machines in separate cavities are in (Fang *et al.*, 2011), by superconducting quantum-interference device qubits in a cavity is presented in (Yang *et al.*, 2008). The scheme for implementing a UQCM in cavity QED with atoms is studied in (Zheng, 2004), by ion trap technique is proposed in (Zheng, 2005), by cavity-assisted atomic collisions is proposed in (Zou *et al.*, 2003), via cavity-assisted interaction is studied in (Fang *et al.*, 2012a). The scheme of quantum cloning of atomic state into two photonic states is presented in (Song and Qin, 2008). The comparison of fidelities of quantum cloning expressed in theory and under experimental conditions is investigated in (Khan and Howell, 2004). The well-accepted theory of fidelity for mixed states can be found in (Josza, 1994).

IV. PROBABILISTIC QUANTUM CLONING

Concerning about the B92 protocol which involves only two non-orthogonal states (Bennett, 1992), we can try to clone it with the largest probability. That is, by measuring a detector, we can make sure that the involved state is cloned perfectly or we know that the cloning process fails. The aim of this quantum cloning is to achieve the optimal probability.

A. Probabilistic quantum cloning machine

While the previous mentioned quantum cloning machines can always succeed, on the same time, the copies cannot be perfect. Duan and Guo (Duan and Guo, 1998a,b, 1999) proposed a different quantum cloning machine: while the coping task can succeed with probability, but if it is successful, we can always obtain perfect copies. This kind of quantum cloning machine is called probabilistic quantum cloning machine.

This quantum cloning machine is useful, in particular, in studying the B92 quantum key distribution protocol (Bennett, 1992). In this QKD protocol, only two non-orthogonal states are used for key distribution so the attack is simply to use a specified quantum cloning machine to clone those two non-orthogonal states. In fact, this is the simplest case for probabilistic quantum cloning machine which is used to copy two linearly independent states $S = \{|\Psi_0\rangle, |\Psi_1\rangle\}$(Duan and Guo, 1998b). The cloning transformation can be proposed as:

$$\begin{aligned} U(|\Psi_0\rangle|\Sigma\rangle|m_p\rangle) &= \sqrt{\eta_0}|\Psi_0\rangle|\Psi_0\rangle|m_0\rangle + \sqrt{1-\eta_0}|\Phi^0_{ABP}\rangle, \\ U(|\Psi_1\rangle|\Sigma\rangle|m_p\rangle) &= \sqrt{\eta_1}|\Psi_1\rangle|\Psi_1\rangle|m_1\rangle + \sqrt{1-\eta_1}|\Phi^1_{ABP}\rangle, \end{aligned} \tag{126}$$

where $|m_p\rangle, |m_0\rangle\rangle, |m_1\rangle$ are ancillary states. The measurements are performed in these states. And the states $|\Phi^0_{ABP}\rangle$ and $|\Phi^1_{ABP}\rangle$ are chosen so that the reduced state of P is orthogonal to $|m_0\rangle$ and $|m_1\rangle$. When the measurements are $|m_0\rangle$ or $|m_1\rangle$, we know the states $S = \{|\Psi_0\rangle, |\Psi_1\rangle\}$ are copied perfectly. Otherwise, the cloning task fails. The probabilities of success are η_0 and η_1 for states $|\Psi_0\rangle$ and $|\Psi_1\rangle$, respectively. If we let $\eta_0 = \eta_1 = \eta$, we know that

$$\eta \leq \frac{1}{1 + |\langle\Psi_0|\Psi_1\rangle|}. \tag{127}$$

This is also a no-cloning theorem: only orthogonal states can be cloned perfectly. And the optimal probabilistic quantum cloning is to let $\eta = 1/(1 + |\langle\Psi_0|\Psi_1\rangle|)$. It is also related with the problem of how to distinguish non-orthogonal quantum states.

The more complicated case is to copy a set of linearly independent states $S = \{|\Psi_0\rangle, |\Psi_1\rangle ..., |\Psi_n\rangle\}$. The form of the probabilistic cloning mahcine is:

$$U(|\Psi_i\rangle|\Sigma\rangle|P_0\rangle) = \sqrt{\gamma_i}|\Psi_i\rangle|\Psi_i\rangle|P_0\rangle + \sum_{j=1}^{n} c_{ij}|\Phi^j_{AB}\rangle|P_j\rangle. \tag{128}$$

$P_0 \dots P_n$ is a set of orthonormal ancilla states. Hence if the measurement result of the ancilla turns out to be P_0, we know the state $|\Psi_i\rangle$ is perfectly cloned, with the probability γ_i. Taking the inner product of different i and j in (128), there's a matrix equation

$$X^{(1)} - \sqrt{\Gamma}X^{(2)}\sqrt{\Gamma} = CC^\dagger \tag{129}$$

where $X^{(k)}_{ij} = \langle\Psi_i|\Psi_j\rangle^k$, $\Gamma = \Gamma^\dagger = diag\{\gamma_1 \dots \gamma_n\}$, $C_{ij} = c_{ij}$. If the input states $|\Psi_i\rangle$s are not linearly independent, $X^{(1)}$ is not positive definite. And for generic positive definite matrix Γ, the right-handed side of (129) is not positive semidefinite, hence the equation is not valid as the matrix $CC^\dagger$ is positive semidefinite. Hence such probabilistic cloning machine only exists for linearly independent states(This result is also confirmed by Hardy and Song using the no-signaling argument(Hardy and Song, 1999)). They then found the existence is equivalent to the positive semidefiniteness of $X^{(1)} - \Gamma$. The result is called the Duan-Guo bound to distinguish linearly independent quantum states(Duan and Guo, 1998a). The $1 \to M$ cloning machine is also easy to formulate, just by adding the number of copies at the right-handed side of (128). Later, Zhang *et al.*(Zhang *et al.*, 2000b) constructed a network using universal quantum logic states realizing this cloning machine.

Later, Azuma *et al.* (Azuma *et al.*, 2005) studied the case with supplementary information, that is, the $|\Sigma\rangle$ at the left-handed side of (128) is state dependent. Li and Qiu (Li and Qiu, 2007) explored the case with two ancilla systems, but it is shown that the performance cannot be improved.

B. A novel quantum cloning machine

For probabilistic cloning machine, Pati (Pati, 1999) explored the possibility that the output state contains all possible copies of the original state. That is, for a set of input states $|\Psi_1\rangle \dots |\Psi_n\rangle$, does there exist a transformation U in the following form:

$$U(|\Psi_i\rangle|\Sigma\rangle|P_0\rangle) = \sum_{j=1}^{M} \sqrt{p_j^{(i)}}|\Psi_i\rangle^{\otimes(j+1)}|0\rangle^{\otimes(M-j)}|P_j\rangle + \sum_{k=M+1}^{N'} \sqrt{f_k^{(i)}}|\Phi_{AB}^k\rangle|P_k\rangle. \tag{130}$$

$|P_1\rangle, \dots, |P_{N'}\rangle$ is a set of orthonormal ancilla states, as usual. In fact, this can be regarded as a superposition of the $1 \to 2, \cdots, 1 \to (M+1)$ cloning machines. From the unitarity constraint, we have

$$\langle\Psi_i|\Psi_j\rangle = \sum_{k=1}^{M} \sqrt{p_k^{(i)}}\langle\Psi_i|\Psi_j\rangle^{k+1}\sqrt{p_k^{(j)}} + \sum_{l=M+1}^{N'} \sqrt{f_l^{(i)} f_l^{(j)}}. \tag{131}$$

This equation can be rewritten as a equation of matrices

$$X^{(1)} = \sum_{k=1}^{M} P_k X^{(k+1)} P_k + \sum_{l=M+1}^{N'} F^{(l)}. \tag{132}$$

Here $P_k = P_k^\dagger = diag\{p_k^{(1)}, \dots, p_k^{(n)}\}$,$X_{ij}^{(k)} = \langle\Psi_i|\Psi_j\rangle^k$ as usual and $F_{ij}^{(l)} = \sqrt{f_l^{(i)} f_l^{(j)}}$. From this relation, they proved if the states are linearly independent, then the equation can be satisfied with positive definite P_ks and F_ls. It's also simple to see the transformation doesn't exist if the set of input state contains a state that is a superposition of other states says $|\Psi\rangle = \sum_j c_j|\Psi_j\rangle$, since we can simply add the $U(|\Psi\rangle|\Sigma\rangle|P_0\rangle) = \sum_j c_j U(|\Psi_j\rangle|\Sigma\rangle|P_0\rangle)$. And from the right-handed side of (130) we can see that it is inconsistent.

Under this framework, the cloning machine of Duan and Guo can be viewed as a special case of $M = 1$, see (Duan and Guo, 1998b).

Later, Qiu (Qiu, 2002) proposed a combination of Pati's probabilistic cloning machine and the approximate cloning machine in the usual sense, which is a more general framework. The condition with supplementary information is also explored, that is, the $|\Sigma\rangle$ at the input side is state dependent. It is found that the probability of success may increase(Qiu, 2006).

C. Probabilistic quantum NOT gate

Similar to the approximate universal NOT gate in the UQCM section in this paper, we can also construct a probabilistic NOT gate under the framework of probabilistic cloning. A $1 \to 2$ probabilistic NOT gate is proposed by Hardy and Song in (citation needed):

$$U(|\Psi_i\rangle|\Sigma\rangle|P_0\rangle) = \sqrt{f}|\Psi_i\rangle|\Psi_i^\perp\rangle|P_0\rangle + \sum_{j=1}^{n} c_{ij}|\Phi_{AB}^j\rangle|P_j\rangle. \tag{133}$$

The input states are $|\Psi_1\rangle, \dots, |\Psi_n\rangle$, as usual. Taking the inner product of different i, j, we get

$$X^{(1)} = fX' + CC^\dagger \tag{134}$$

where $X'_{ij} = \langle\Psi_i|\Psi_j\rangle\langle\Psi_i^\perp|\Psi_j^\perp\rangle$ and other notation is same as above. If the input states are linearly independent, then the Gram matrix at the left-handed side of above equation is positive definite. Hence for a sufficiently small f, we can guarantee $CC^\dagger$ is also positive semidefinite. So such a cloning machine always exists. As a simple example, we consider the case $n = 2, a_{11} = a_{21} = \sqrt{1-f}, a_{12} = a_{22} = 0$, then (133) can be written as:

$$\begin{aligned} |\Psi_1\rangle &\to \sqrt{f}|\Psi_1\rangle|\Psi_1^\perp\rangle|P_0\rangle + \sqrt{1-f}|\Phi_{AB}\rangle|P_1\rangle \\ |\Psi_2\rangle &\to \sqrt{f}|\Psi_2\rangle|\Psi_2^\perp\rangle|P_0\rangle + \sqrt{1-f}|\Phi_{AB}\rangle|P_1\rangle. \end{aligned} \tag{135}$$

In this case, we have a constraint of f:

$$f \le \frac{1 - |\langle\Psi_1|\Psi_2\rangle|}{1 - |\langle\Psi_1|\Psi_2\rangle||\langle\Psi_1^\perp|\Psi_2^\perp\rangle|} = \frac{1}{1 + |\langle\Psi_1|\Psi_2\rangle|} \tag{136}$$

which is identical to the Duan and Guo case (Duan and Guo, 1998b). Li *et al.* (Li *et al.*, 2007) extended the above case to the case where the output state contains all of $|\Psi\rangle|\Psi^\perp\rangle, |\Psi\rangle|\Psi^\perp\rangle^{\otimes 2}, \dots, |\Psi\rangle|\Psi^\perp\rangle^{\otimes M}$.

D. Other developments and related topics

Fiurášek (Fiurášek, 2004) used the technique described in the "Singlet Monogamy" subsection in the UQCM part to analyze the optimality of probabilistic cloning machine. Li *et al.* (Li *et al.*, 2009) investigated the broadcasting of mixed state using probabilistic cloning machine. Wang and Yang (Wang and Yang, 2009b) studied the optimal probabilistic ancilla-free phase-covariant qudit telecloning machine. Jimenez *et al.* studied the probabilistic cloning of three symmetric states (Jimenez *et al.*, 2010a) and equidistant states (Jimenez *et al.*, 2010b). Zhang *et al.* studied probabilistic cloning of qubits with real parameters (Zhang *et al.*, 2010a) and the relation between probabilistic cloning and state discrimination (Zhang *et al.*, 2010b). The relation between this cloning machine and states discrimination is also studied in (Feng *et al.*, 2005) and in (Chefles and Barnett, 1998). The minimum-error discrimination between mixed states of the ambiguous case is studied in (Qiu, 2008). The optimal unambiguous discrimination of two density matrices is studied in (Raynal and Lutkenhaus, 2005). The optimal observables for minimum-error state discrimination is studied in (Nuida *et al.*, 2010). By homodyne detection, distinguishing two single-mode Gaussian states is studied in (Nha and Carmichael, 2005). It is also shown that according to Wigner-Araki-Yanase theorem that the repeatability and distinguishability cannot be reached simultaneously (Miyadera and Imai, 2006b), also to distribute a quantum state to a coupled two subsystems, the strength of interaction should be above a threshold (Miyadera and Imai, 2006a). Then Mishra (Mishra, 2012) investigated the unambiguous discrimination of two squeezed states using probabilistic cloning. The scheme to implement probabilistic cloning of qubits via twin photons is proposed in (Araneda *et al.*, 2012). The realization scheme by GHZ states is proposed by Zhang *et al.* in (Zhang *et al.*, 2000a). The assisted cloning is proposed by Pati in (Pati, 2000). Experimentally, the accuracy of quantum state estimation is studied which is also compared with asymptotic lower bound obtained theoretically by Cramer-Rao inequality (Usami *et al.*, 2003). The probabilistic quantum cloning experimentally realized in NMR system is reported in (Chen *et al.*, 2011). By generalizing the probabilistic cloning to state amplification, the experimental heralded amplification of the photon polarized state and entanglement distillation are reported in (Xiang *et al.*, 2010) and (Kocsis *et al.*, 2013).

V. PHASE-COVARIANT AND STATE-DEPENDENT QUANTUM CLONING

In last section, we studied the quantum cloning machines which are universal. That is the case that the input states are arbitrary or we know nothing about the input state. Practically, it is possible that we already know partial information of the input state. The point is whether this partial information is helpful or not for us to obtain a better fidelity in quantum cloning. In this section, we will show that depending on specified input states, we can design some quantum cloning machines which perform better for those restricted input states than that the universal cloning machines.

On the other hand, one of the most important applications of quantum cloning is to analyze the security of quantum key distribution protocols. In security analysis, the quantum states transfer through a quantum channel. We suppose that this quantum channel is controlled by the eavesdropper who is generally named as Eve. Eve can perform any operations which is allowed by quantum mechanics. One direct attack is the "receive-measure-resend" attack where "measure" can be supposed to be a quantum operation. However, quantum mechanics states that non-orthogonal quantum states cannot be distinguished perfectly. So the measured results will in general not be perfect and thus the obtained measurement result is not the original sent state. This will induce inevitable errors which can be detected by public discussions between the legitimated sender and receiver, Alice and Bob, in QKD.

Eve can choose freely her attack schemes. The quantum cloning machines provide a quantum scheme of eavesdropping attack. We just assume that the Eve has an appropriate quantum cloning machine. By quantum cloning, Eve can keep one copy of the transferring state and send another copy to the legitimate receiver, Bob. Now Eve and Bob both have copies of the sending state. By this process, we can find how much information can be obtained by Eve, and on the other hand, how much errors are induced by this attack. This provides a security analysis of QKD. In this eavesdropping, Eve intends to get some information secretly between Alice and Bob's communication and wish to make the least possibility to be detected. So the optimal quantum cloning machine is required. Based on different QKD protocols, various cloning machines are designed specially. The universal quantum cloning machines studied in the previous sections themselves might be optimal. But it may not be optimal for the quantum states involved in a special QKD protocol. So the state-dependent quantum cloning machines are necessary. In this section, we will give all the examples of state-dependent cloning.

A. Quantum key distribution protocols

In this subsection, we intend to refer some quantum key distribution protocols and show how the eavesdropper attacks them. Each protocol may lead to a special kind state-dependent cloning machine. Initial protocols are based simply on 2-dimension system and later they are generalized to higher-dimension. Next, we present in detail the well-known BB84 protocol (Bennett and Brassard, 1984) and briefly its generalizations. An earlier review of QKD is in (Gisin *et al.*, 2002).

1. BB84 protocol (Bennett and Brassard, 1984) uses two sets of orthogonal 2-level states and intersection angle in Bloch-sphere between different sets is 90°. They can be written as following, see FIG.2,

$$\begin{aligned} &|0\rangle, |1\rangle, \\ &\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{137}$$

   Note that by operating a unitary transformation, characteristics of these states remain unchanged. Therefore, we may also use the following four states in BB84 protocol which are still two sets of orthogonal 2-level states with 90° intersection angle, also see all those states in FIG.2.

$$\begin{aligned} &\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \\ &\frac{1}{\sqrt{2}}(|0\rangle \pm \mathrm{i}|1\rangle). \end{aligned} \tag{138}$$

   In BB84 protocol, Alice sends one of these four qubits to Bob through a certain quantum channel which is controlled by Eve. After receiving the qubit, Bob measures the obtained qubit with one of the two bases randomly. After Bob has finished his measurement, Alice would announce the bases of each qubits. If their bases coincidence, Bob's measurement result is surely correct. Alice and Bob will share a common secrete key.

If sending basis and the measurement basis are different, they simply discord this bit of information. Also they may use some qubits as the checking qubits to find out the error rate introduced by the quantum channel. They can suppose that all errors are caused by Eve's attack.

The eavesdropper, Eve, will capture the qubits in the quantum channel and clone them. She remains one part to copies and still sends the other part to Bob in the quantum channel. As soon as Alice broadcasts the bases, Eve measures her own qubits sequentially to derive the information sent between Alice and Bob.

This BB84 protocol is proved to be unconditional secure and the security is based on principles of quantum mechanics. The security proofs of BB84 protocol are given by several groups, for example Mayers (Mayer, 2001), Lo and Chau (Lo and Chau, 1999), Shor and Preskil (Shor and Preskill, 2000). We remark that Ekert proposed a QKD strategy based on the non-locality of quantum mechanics (Ekert, 1991) which is the same of the BB84 protocol.

2. B92(Bennett, 1992) is a protocol which uses any two non-orthogonal states. Tamaki *et al.* (Tamaki *et al.*, 2003) provide the security proof of this protocol. In this review, we suppose those two states take the form,

$$\frac{1}{\sqrt{2}}(|0\rangle + \mathrm{e}^{\mathrm{i}\phi_k}|1\rangle), k = 1, 2. \tag{139}$$

3. BB84 protocol can be generalized to 6-state protocol(Bruß, 1998). The six states involved in this protocol are BB84 states plus two more states as shown in Eq.(124). Interestingly, the optimal cloning of those six states is the universal quantum cloning machine as already shown in previous sections.

4. For higher-dimensional case, the QKD protocols can use 2-basis or $d+1$-basis in a d-level system as studied by Cerf *et al.* (Cerf *et al.*, 2002a).

5. In d-dimension, there are altogether $d+1$ mutually unbiased bases (MUB), provided d is prime. Any $(g+1)$-basis from those MUBs, $g = 1, 2, ..., d$, can actually be used for QKD (Xiong *et al.*, 2012). Here, we briefly give the definition of MUB, $\{|i\rangle\}$ and $\{|\tilde{i}^{(k)}\rangle\}$ $(k = 0, 1, ..., d-1)$, they are expressed as:

$$|\tilde{i}^{(k)}\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\omega^{i(d-j)-ks_j}|j\rangle, \tag{140}$$

with $s_j = j + ... + (d-1)$ and $\omega = e^{i\frac{2\pi}{d}}$. These states satisfy the condition, $|\langle\tilde{i}^{(k)}|\tilde{l}^{(j)}\rangle| = \delta_{kj}\delta_{il} + \frac{1}{\sqrt{d}}(1-\delta_{kj})$. States in different set of bases are mutually unbiased.

6. Basing on the characteristics of MUB, we can design a retrodiction protocol using method of mean king game. This special protocol, different from BB84 or other QKD protocols, shows that Bob has a 100% successful measurement scheme in comparison with the $1/(g+1)$ successful measurement in such as BB84 protocols. Here we remark that quantum memory is not available for Bob. We will present a detailed analysis of this retrodiction protocol.

B. General state-dependent quantum cloning

As to the above QKD protocols, universal quantum cloning machine is sure to work well, but not surely to be the optimal one. Thus if we need a higher quality of the output from the cloning machine, a state-dependent cloning machine is needed. In fact, each protocol corresponds to a special kind of state-dependent cloning machine based on the given ensembles of states.

Let us firstly consider a general case based on two equatorial states. Obviously, it is equivalent to the B92 protocol (Bennett, 1992). To be non-trivial and satisfy the B92 protocol, these states are nonorthogonal. The cloning machine is designed to clone only these two states optimally and equally well without considering other states on the Bloch sphere. This problem is studied in (Bruß *et al.*, 1998a).

The quantum cloning machine takes a completely unknown 2-level state $|\psi\rangle$ and makes two output qubits. Each output state is described by a reduced density matrix with the following form,

$$\rho = \eta|\psi\rangle\langle\psi| + (1-\eta)\frac{\mathbb{I}}{2}. \tag{141}$$

Here, η described the shrinking of the initial Bloch vector $\vec{s}$ corresponding to the density matrix $|\psi\rangle\langle\psi|$. In other words, the output state is

$$\rho = \frac{\mathbb{I} + \eta \vec{s} \cdot \vec{\sigma}}{2},$$

with the input state being

$$|\psi\rangle\langle\psi| = \frac{\mathbb{I} + \vec{s} \cdot \vec{\sigma}}{2}. \tag{142}$$

We assume that any quantum cloning machine satisfies the following reasonable conditions according to requirement of all QKD protocols: First, $\rho_1 = \rho_2$, which is called symmetry condition. Second, $F = Tr(\rho_\psi \rho_1) = const.$, which is called isotropy condition meaning that the fidelity between each output and the input does not depend on the specified form of the input. Stronger condition $\vec{s_1} = \eta_\psi \vec{\psi}$ is required by orientation invariance of the Bloch vector. It is obvious that when the last condition is satisfied, the second will be satisfied.

Next let us investigate the explicit form of the quantum cloning machine. Bruß *et al.* (Bruß *et al.*, 1998a) make a general ansatz for the unitary transformation U performed by the cloning machine. They are,

$$U|0\rangle|0\rangle|X\rangle = a|00\rangle|A\rangle + b_1|01\rangle|B_1\rangle + b_2|10\rangle|B_2\rangle + c|11\rangle|C\rangle, \tag{143}$$

$$U|1\rangle|0\rangle|X\rangle = \tilde{a}|11\rangle|\tilde{A}\rangle + \tilde{b_1}|10\rangle|\tilde{B_1}\rangle + \tilde{b_2}|01\rangle|\tilde{B_2}\rangle + \tilde{c}|00\rangle|\tilde{C}\rangle. \tag{144}$$

where $|X\rangle$ is an input ancilla. And $|A\rangle, |B_i\rangle, ...$ denote output ancilla states. Ancilla states may have any dimension but are required to be normalized. There are several constraints for these parameters. Thanks to the unitarity of the cloning transformation, the complex parameters $a, b_i, c...$ satisfy the normalization conditions:

$$\begin{aligned} |a|^2 + |b_1|^2 + |b_2|^2 + |c|^2 = 1, \\ |\tilde{a}|^2 + |\tilde{b_1}|^2 + |\tilde{b_2}|^2 + |\tilde{c}|^2 = 1, \end{aligned} \tag{145}$$

and the orthogonality condition:

$$a^* \tilde{c} \langle A|\tilde{C}\rangle + b_2^* \tilde{b_1} \langle B_2|\tilde{B_1}\rangle + b_1^* \tilde{b_2} \langle B_1|\tilde{B_2}\rangle + c^* \tilde{a} \langle C|\tilde{A}\rangle = 0. \tag{146}$$

Assume that the cloning machine works in symmetric subspace, more relations are derived

$$\begin{aligned} |b_1| = |b_2|, \quad |\tilde{b_1}| = |\tilde{b_2}|, \\ |\langle B_1|\tilde{B_2}\rangle| = |\langle B_2|\tilde{B_1}\rangle|, \quad |\langle B_1|\tilde{B_1}\rangle| = |\langle B_2|\tilde{B_2}\rangle|, \end{aligned} \tag{147}$$

and

$$\begin{aligned} ab_1^* \langle B_1|A\rangle + c^* b_2 \langle C|B_2\rangle = ab_2^* \langle B_2|A\rangle + c^* b_1 \langle C|B_1\rangle, \\ \tilde{b_1^*} a \langle \tilde{B_1}|A\rangle + \tilde{a}^* b_1 \langle \tilde{A}|B_1\rangle = \tilde{b_2} a \langle \tilde{B_2}|A\rangle + \tilde{a}^* b_2 \langle \tilde{A}|B_2\rangle, \\ b_1^* \tilde{c} \langle B_1|\tilde{C}\rangle + c^* \tilde{b_1} \langle C|B_1\rangle = b_2^* \tilde{c} \langle B_2|\tilde{C}\rangle + c^* \tilde{b_2} \langle C|\tilde{B_2}\rangle. \end{aligned} \tag{148}$$

Moreover, letting shrink factor remaining constant ratio within each direction in Bloch sphere, one has,

$$\frac{s_{1_x}}{s_{\psi_x}} = \frac{s_{1_y}}{s_{\psi_y}} = \frac{s_{1_z}}{s_{\psi_z}} = \eta_\psi. \tag{149}$$

Applied in the transformation, we may derive further constraints:

$$\begin{aligned} & |a|^2 - |c|^2 = |\tilde{a}|^2 - |\tilde{c}|^2 \\ & |a|^2 - |c|^2 = Re[\tilde{b_1}^* a \langle \tilde{B_1}|A\rangle + \tilde{a}^* b_1 \langle \tilde{A}|B_1\rangle], \\ & Im[\tilde{b_1}^* a \langle \tilde{B_1}|A\rangle + \tilde{a}^* b_1 \langle \tilde{A}|B_1\rangle] = 0, \\ & b_1^* \tilde{c} \langle B_1|\tilde{C}\rangle + c^* \tilde{b_1} \langle C|\tilde{B_1}\rangle = 0, \\ & b_2^* a \langle B_2|A\rangle + c^* b_1 \langle C|B_1\rangle = 0, \\ & \tilde{b_2}^* \tilde{a} \langle \tilde{B_2}|\tilde{A}\rangle + \tilde{c}^* \tilde{b_1} \langle \tilde{C}|\tilde{B_1}\rangle = 0, \\ & \tilde{c}^* a \langle \tilde{C}|A\rangle - \tilde{a}^* c \langle \tilde{A}|C\rangle = 0, \\ \text{and symmetrically,} \quad & 1 \leftrightarrow 2. \end{aligned} \tag{150}$$

Here, notation $1 \leftrightarrow 2$ indicates the above constraints changing indices 1 with 2 according to the symmetry condition.

Our task is to maximize the shrinking factor η with its explicit form taken as,

$$\eta = |a|^2 - |c|^2. \tag{151}$$

The fidelity which is defined as

$$F = Tr(\rho_1 |\psi\rangle\langle\psi|) = \frac{1}{2}(1 + \vec{s_1} \cdot \vec{s_\psi}) \tag{152}$$

is related to the shrinking factor as

$$F = \frac{1}{2}(1 + \eta). \tag{153}$$

Note that that this relationship between fidelity and shrinking factor holds only for pure states. The study of mixed state has already been presented in the previous sections. The above discussions are regardless of the specified QKD protocols.

C. Quantum cloning of two non-orthogonal states

Next, we will consider the situation of B92 protocol in which only two qubits are required to be cloned. Now, we firstly prove that ancilla is necessary in our cloning machine. Without ancilla, we could write down constraints as: $|a|^2 - |c|^2 = |\tilde{a}|^2 - |\tilde{c}|^2$, $|a|^2 - |c|^2 = Re[\tilde{b_1}^* a + \tilde{a}^* b_1]$, $b_2^* a + c^* b_1 = 0$, and $\tilde{b_2}^* \tilde{a} + \tilde{c}^* \tilde{b_1} = 0$. Adding symmetric ansatz, we have $|b_1| = |b_2| = |b|$ and $|\tilde{b_1}| = |\tilde{b_2}| = |\tilde{b}|$.

From these constraints we would have four possible results: (a),$|a| = |c|$ and $|\tilde{a}| = |\tilde{c}|$, (b), $|a| = |c|$ and $|\tilde{b}| = 0$, (c), $|b| = 0$ and $|\tilde{a}| = |\tilde{c}|$, and (d), $|b| = 0$, and $|\tilde{b}| = 0$. For each case, we have $\eta = 0$ which seems meaningless. Consequently, it is impossible to generate a symmetric quantum cloning machine without ancilla.

In the following, we will explicitly give the form of the quantum cloning machine and the fidelity in this case. Assume two pure states in a two-dimensional Hilbert space with expressions:

$$|a\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle, \tag{154}$$

$$|b\rangle = \sin\theta|1\rangle + \cos\theta|0\rangle, \tag{155}$$

where θ varying from 0 to $\pi/4$. Define $S = \langle a|b\rangle = \sin 2\theta$. We may imagine that the fidelity only dependents on S because we could transform every 2 states into the above form by only unitary operation without influence the fidelity.

Since there are too many constraints to give strict algebraic calculations, we utilize the symmetry in the B92 protocol to simplify the calculations. Performing an unitary operator U on the input states, we define final states $|\alpha\rangle$ and $|\beta\rangle$ as

$$|\alpha\rangle = U|a\rangle|0\rangle, |\beta\rangle = U|b\rangle|0\rangle. \tag{156}$$

Since U is an unitary transformation, we could derive

$$\langle\alpha|\beta\rangle = \langle a|b\rangle = \sin 2\theta = S. \tag{157}$$

Using global fidelity F_g to evaluate the quantum cloning, which is defined as

$$F_g = \frac{1}{2}(|\langle\alpha|aa\rangle|^2 + |\langle\beta|bb\rangle|^2) \tag{158}$$

Certainly, optimal cloning machine needs that both $|\alpha\rangle$ and $|\beta\rangle$ lying in the space spanned by vectors $|aa\rangle$ and $|bb\rangle$. Without complicated calculations, we would obtain maximal global fidelity as

$$F_g = \frac{1}{4}(\sqrt{1 + \sin^2 2\theta}\sqrt{1 + \sin 2\theta} + \cos 2\theta\sqrt{1 - \sin 2\theta})^2. \tag{159}$$

Additionally, we are also interested with the local fidelity of each output qubit with the input one, which is defined as

$$F_l = Tr[\rho_\alpha |a\rangle\langle a|]. \tag{160}$$

The explicit result is,

$$F_{l,1} = \frac{1}{2}[1 + \frac{1-S^2}{\sqrt{1+S^2}} + \frac{S^2(1+S)}{1+S^2}]. \tag{161}$$

We may notice that it is larger than 5/6. That is to say, for this protocol, state-dependent cloning machine works better than UQCM as expected. It is also noticed that the Bloch vector not only shrinks but also makes a rotation with a state-dependent angle ϑ:

$$\vartheta = \arccos[\frac{1}{|\vec{s}|}\frac{\cos 2\theta}{\sqrt{1+\sin^2 2\theta}}] - 2\theta. \tag{162}$$

This is caused by that one constraint presented previously is released.

We should emphasize that this result is derived under the request of maximum global fidelity rather than maximum local fidelity. When we only need a better state-dependent cloning machine locally, we may have different consequences. And the fidelity is given by:

$$F_{l,3} = \frac{1}{2} + \frac{\sqrt{2}}{32S}(1+S)(3-3S+\sqrt{1-2S+9S^2}) \times \sqrt{-1+2S+3S^2+(1-S)\sqrt{1-2S+9S^2}}. \tag{163}$$

Moreover, it could be tested that the minimum value $F_{l,3} \approx 0.987$ is derived when $S = 1/2$. And when $S = 0$ and $S = 1$, one finds $F = 1$ as expected.

In addition, we should note that different concerning in the eavesdropping would lead to variant results. In B92 protocol, direct cloning is not the most advisable action for Eve if she wishes to be most surreptitious. In fact, Eve's main purpose is not to clone the quantum information which is embodied in the two nonorthogonal quantum states, but rather to optimize the trade-off between obtaining most classical information versus making the least disturbance on the original qubit(Fuchs and Peres, 1996). We may name it the optimal eavesdropping which is different from optimal cloning. In (Bruß *et al.*, 1998a), fidelity for optimal eavesdropping is expressed as

$$F_{l,2} = \frac{1}{2} + \frac{\sqrt{2}}{4}\sqrt{(1-2S^2+2S^3+S^4)+(1-S^2)\sqrt{(1+S)(1-S+3S^2-S^3)}}. \tag{164}$$

Note that, for all S, $F_{l,2} \geq F_{l,3}$.

Here we have a short summary, the general state-dependent cloning machine works better than UQCM when applied to a certain number of states. We give the special case of two nonorthogonal pure states. It is obviously that, if we know the ensemble of states used in one QKD protocol, state-dependent cloning machine can be designed accordingly. Besides for QKD protocols, various quantum machines themselves are of fundamental interests. As an extension of B92 protocol, Koashi and Imoto considered the quantum cryptography by two mixed states (Koashi and Imoto, 1996).

D. Phase-covariant quantum cloning: economic quantum cloning for equatorial qubits

In this subsection, we will discuss quantum cloning machine for BB84 states, which is first studied in (Bruß *et al.*, 2000a). For convenience, we will also refer those four states $\{(|0\rangle \pm |1\rangle)/\sqrt{2}, (|0\rangle \pm i|1\rangle)/\sqrt{2}\}$ as the BB84 states. In fact, the cloning machine of BB84 states is proved to be able to copy all equatorial states optimally. It has a higher fidelity than that of the UQCM. Moreover, this kind of quantum cloning machine is able to work without the help of the ancilla states. It is thus the economic quantum cloning.

It is interesting to find that any quantum cloning machine that clones BB84 states equally well will also clone equatorial states with the same fidelity. We know that the equatorial qubits are located on the equator of the Bloch sphere which take the form, $|\psi(\phi)\rangle = (|0\rangle + e^{i\phi}|1\rangle)/\sqrt{2}$ see FIG.4. Since each output qubit can be represented as the mixture of input state and the completely mixed state and the corresponding fidelity does not depend on the phase ϕ, this kind of cloning machine is "phase covariant". It is named generally as the phase-covariant quantum cloning machine.

Consider a completely positive map T that could clone optimally the four states of BB84. Perform T on those states would lead to approximate result:

$$T[|\pm x\rangle\langle \pm x|] = \eta|\pm x\rangle\langle \pm x| + (1-\eta)\frac{\mathbb{I}}{2}, \tag{165}$$

$$T[|\pm y\rangle\langle \pm y|] = \eta|\pm y\rangle\langle \pm y| + (1-\eta)\frac{\mathbb{I}}{2}. \tag{166}$$

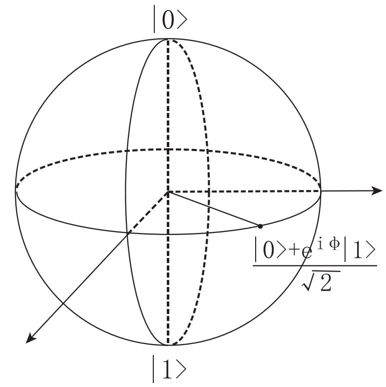


FIG. 4 The equatorial qubits are qubits which are located on the equtor of the Bloch sphere. The optimal cloning machine for those states is the phase-covariant quantum cloning machine. This machine is also optimal for cloning BB84 like states.

On the other hand, equatorial states could be written as

$$|\psi(\phi)\rangle\langle\psi(\phi)| = \frac{1}{2}(\mathbb{I} + \cos\phi\sigma_x + \sin\phi\sigma_y). \tag{167}$$

This is the qubits in $x-y$ equator. Similarly we have qubits in $x-z$ equator such as BB84 states and in $y-z$ equator. Perform linear operation T on it and consider $T(\mathbb{I}) = \mathbb{I}$, we derive

$$T[|\psi(\phi)\rangle\langle\psi(\phi)|] = \eta|\psi(\phi)\rangle\langle\psi(\phi)| + (1-\eta)\frac{\mathbb{I}}{2} \tag{168}$$

The shrinking factor η remains unchanged. Therefore, we could conclude that optimal cloning machine performed for the BB84 states is equivalent to phase covariant cloning machine.

Next, we release the above constraint that the single output qubit takes the scalar form (168). We only need that the fidelity does not depend on the phase parameter ϕ in quantum cloning. We fist consider the economic case, which is accomplished without ancilla. Phase-covariant quantum cloning machine is presented in the following as proposed by Niu and Griffiths (Niu and Griffiths, 1999),

$$\begin{aligned} &|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle, \\ &|1\rangle|0\rangle \rightarrow \cos\eta|1\rangle|0\rangle + \sin\eta|0\rangle|1\rangle, \end{aligned} \tag{169}$$

where $\eta \in [0, \pi/2]$ means the asymmetry between the two output states. And when $\eta = \pi/4$ the two output states are equivalent, corresponding to the symmetric case.

For any equatorial state $|\psi(\phi)\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)$ which is the input state, we have

$$|\psi(\phi)\rangle|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + \cos\eta e^{i\phi}|10\rangle + \sin\eta e^{i\phi}|01\rangle). \tag{170}$$

So we could easily obtain the reduced matrix of each states,

$$\begin{aligned} \rho_A &= Tr_B(|\psi(\phi)\rangle\langle\psi(\phi)|) \\ \rho_B &= Tr_A(|\psi(\phi)\rangle\langle\psi(\phi)|). \end{aligned} \tag{171}$$

Then, as to any equatorial state $|\psi(\phi)\rangle$, we have fidelity defined as $F = \langle\psi|\rho|\psi\rangle$:

$$F_A = \frac{1}{2}(1 + \cos\eta), \tag{172}$$

$$F_B = \frac{1}{2}(1 + \sin\eta). \tag{173}$$

Obviously, fidelities are independent of ϕ as expected. Particularly, for symmetric case $\eta = \pi/4$, the fidelity is

$$F = 1/2 + 1/\sqrt{8} \approx 0.85355 > \frac{5}{6} \approx 0.833333. \tag{174}$$

In other words, phase covariant cloning machine behaves better than UQCM in cloning equatorial states. Phase-covariant quantum cloning machine can also be realized with ancillary states in a different form. The related results of phase cloning can be found in (Acín *et al.*, 2004b; Bruß *et al.*, 2000a; Durt and Du, 2004; Griffiths and Niu, 1997). The experimental implementation of this scheme is reported in optics system and nuclear magnetic resonance system (Cernoch *et al.*, 2006; Du *et al.*, 2005).

E. One to many phase-covariant quantum cloning machine for equatorial qubits

For quantum cloning, we are always interested in the case that multi-copies created from some fewer identical input states. The simplest extension of $1 \to 2$ is one to many quantum cloning, i.e. $1 \to M$ phase-covariant quantum cloning. Based on the cloning transformations similar to the UQCM (Gisin and Massar, 1997), for arbitrary equatorial qubits, $|\Psi\rangle = (|\uparrow\rangle + e^{i\phi}|\downarrow\rangle)/\sqrt{2}$, it is assumed that the cloning transformations take the following form (Fan *et al.*, 2001b),

$$\begin{aligned} U_{1,M}|\uparrow\rangle \otimes R &= \sum_{j=0}^{M-1} \alpha_j |(M-j)\uparrow, j\downarrow\rangle \otimes R_j, \\ U_{1,M}|\downarrow\rangle \otimes R &= \sum_{j=0}^{M-1} \alpha_{M-1-j} |(M-1-j)\uparrow, (j+1)\downarrow\rangle \otimes R_j, \end{aligned} \tag{175}$$

where R denotes the initial state of the copy machine and $M-1$ blank copies, R_j are orthogonal normalized states of the ancillary (ancilla), and $|(M-j)\psi, j)\psi_\perp\rangle$ denotes the symmetric and normalized state with $M-j$ qubits in state ψ and j qubits in state $\psi_\perp$. We already know the result of universal case: For arbitrary input state, the case $\alpha_j = \sqrt{\frac{2(M-j)}{M(M+1)}}$ is the optimal $1 \to M$ universal quantum cloning (Gisin and Massar, 1997).

Next we consider the case that the input states being restricted to the equatorial qubits. It is assumed that phase-covariant transformations satisfy some properties: it possesses the orientation invariance of the Bloch vector and that the output states are in symmetric subspace which naturally ensure that we have identical copies. The unitarity and the normalization is satisfied by $\sum_{j=0}^{M-1} \alpha_j^2 = 1$. We now wish that the optimal phase-covariant cloning machine can be achieved. Let us see fidelity which is found to take the form,

$$F = \frac{1}{2}[1 + \eta(1, M)], \tag{176}$$

where

$$\eta(1, M) = \sum_{j=0}^{M-1} \alpha_j \alpha_{M-1-j} \frac{C_{M-1}^j}{\sqrt{C_M^j C_M^{j+1}}}. \tag{177}$$

From this result, it is straightforward to examine two special cases, $M = 2, 3$. For $M = 2$, we have $\alpha_0^2 + \alpha_1^2 = 1$ and $\eta(1, M) = \sqrt{2}\alpha_0\alpha_1$. In case $\alpha_0 = \alpha_1 = 1/\sqrt{2}$, the fidelity achieves the maximum. For $M = 3$, we have $\alpha_0^2 + \alpha_1^2 + \alpha_2^2 = 1$, and

$$\eta(1, 3) = \frac{2}{3}\alpha_1^2 + \frac{2}{\sqrt{3}}\alpha_0\alpha_2. \tag{178}$$

For $\alpha_0 = \alpha_2 = 0, \alpha_1 = 1$, we have $\eta(1, 3) = \frac{2}{3}$, which is the optimal value and it reproduces the case of quantum triplicator for $x - y$ equatorial qubits as presented below,

$$\begin{aligned} |\uparrow\rangle &\to \frac{1}{\sqrt{3}}(|\uparrow\uparrow\downarrow\rangle + |\uparrow\downarrow\uparrow\rangle + |\downarrow\uparrow\uparrow\rangle), \\ |\downarrow\rangle &\to \frac{1}{\sqrt{3}}(|\downarrow\downarrow\uparrow\rangle + |\downarrow\uparrow\downarrow\rangle + |\uparrow\downarrow\downarrow\rangle). \end{aligned} \tag{179}$$

Note that the fidelity of this quantum triplicator is 5/6 which is the same as the $1 \to 2$ UQCM.

We next review the result of 1 to M phase-covariant quantum cloning transformations. When M is even, we suppose $\alpha_j = \sqrt{2}/2, j = M/2 - 1, M/2$ and $\alpha_j = 0$, otherwise. When M is odd, we can suppose $\alpha_j = 1, j = (M-1)/2$ and

$\alpha_j = 0$, otherwise. The corresponding fidelities are $F = \frac{1}{2} + \frac{\sqrt{M(M+2)}}{4M}$ for M is even, and $F = \frac{1}{2} + \frac{(M+1)}{4M}$ for M is odd. The explicit cloning transformations have already been presented in (175).

The above fidelities for $M = 2, 3$ cases are optimal, we next prove that for general M, the fidelities achieve the maximum as well. The method introduced in (Gisin and Massar, 1997) can be also applied in this phase-covariant case. For convenience, we consider the general N to M cloning transformation. By expansion, the N identical input states for equatorial qubits can be written as,

$$|\Psi\rangle^{\otimes N} = \sum_{j=0}^{N} e^{ij\phi}\sqrt{C_N^j}|(N-j)\uparrow, j\downarrow\rangle. \tag{180}$$

The most general N to M quantum cloning machine for equatorial qubits is expressed as

$$|(N-j)\uparrow, j\downarrow\rangle \otimes R \rightarrow \sum_{k=0}^{M} |(M-k)\uparrow, k\downarrow\rangle \otimes |R_{jk}\rangle, \tag{181}$$

where R still denotes the $M-N$ blank copies and the initial state of the cloning machine, and $|R_{jk}\rangle$ are unnormalized final states of the ancilla. By using the unitarity condition, we know,

$$\sum_{k=0}^{M} \langle R_{j'k}|R_{jk}\rangle = \delta_{jj'}. \tag{182}$$

The fidelity then takes the form

$$F = \langle\Psi|\rho^{out}|\Psi\rangle = \sum_{j',k',j,k} \langle R_{j'k'}|R_{jk}\rangle A_{j'k'jk}, \tag{183}$$

where ρ^{out} is the density operator of each output qubit by taking partial trace over $M-1$ output qubits with only one qubit left. We impose the condition that the output density operator has the property of Bloch vector invariance, and find the following for $N = 1$,

$$\begin{aligned} A_{j'k'jk} &= \frac{1}{4}\{\delta_{j'j}\delta_{k'k} + (1-\delta_{j'j})[\delta_{k',(k+1)}\frac{\sqrt{(M-k)(k+1)}}{M} \\ &\quad +\delta_{k,(k'+1)}\frac{\sqrt{(M-k')(k'+1)}}{M}]\}, \end{aligned} \tag{184}$$

where $j, j' = 0, 1$ for case $N = 1$. The optimal fidelity of this cloning machine for equatorial qubits corresponds to the maximal eigenvalue λ_{max} of matrix A by $F = 2\lambda_{max}$ (Gisin and Massar, 1997). The matrix A (184) is a block diagonal matrix with block B given by,

$$B = \frac{1}{4}\begin{pmatrix} 1 & \frac{\sqrt{(M-k)(k+1)}}{M} \\ \frac{\sqrt{(M-k)(k+1)}}{M} & 1 \end{pmatrix}. \tag{185}$$

Thus we now can confirm that the optimal fidelities of 1 to M cloning machine for equatorial qubits takes the form,

$$F = 2\lambda_{max} = \begin{cases} \frac{1}{2} + \frac{\sqrt{M(M+2)}}{4M}, & \text{M is even,} \\ \frac{1}{2} + \frac{(M+1)}{4M}, & \text{M is odd.} \end{cases} \tag{186}$$

Explicitly, the corresponding $1 \rightarrow M$ optimal phase-covariant quantum cloning can be written as:

1. M is even, suppose $M = 2L$, we have

$$\begin{aligned} |\uparrow\rangle &\rightarrow \frac{\sqrt{2}}{2}|(L+1)\uparrow, (L-1)\downarrow\rangle \otimes R_0 + +\frac{\sqrt{2}}{2}|L\uparrow, L\downarrow\rangle \otimes R_1, \\ |\downarrow\rangle &\rightarrow \frac{\sqrt{2}}{2}|L\uparrow, L\downarrow\rangle \otimes R_0 + \frac{\sqrt{2}}{2}|(L-1)\uparrow, (L+1)\downarrow\rangle \otimes R_1. \end{aligned} \tag{187}$$

2. M is odd, suppose $M = 2L + 1$, we have

$$
\begin{aligned}
|\uparrow\rangle &\rightarrow |(L+1)\uparrow, L\downarrow\rangle, \\
|\downarrow\rangle &\rightarrow |L\uparrow, (L+1)\downarrow\rangle.
\end{aligned} \tag{188}
$$

Note that those transformations (187) have ancillary states R_0, R_1. The simplest economic case without these ancillary states has been presented in (169). The general economic case equivalent with Eq.(187) can be written as,

$$
\begin{aligned}
|\uparrow\rangle &\rightarrow |(L+1)\uparrow, (L-1)\downarrow\rangle \\
|\downarrow\rangle &\rightarrow |L\uparrow, L\downarrow\rangle.
\end{aligned} \tag{189}
$$

The optimal phase-covariant quantum cloning for the general $N \rightarrow M$ case still seems elusive, some related results and the phase-cloning of qutrits can be found in (D'Ariano and Macchiavello, 2003). The one to three phase-covariant quantum cloning is realized in optics system (Sciarrino and De Martini, 2005).

F. Phase quantum cloning: comparison between economic and non-economic

It seems that phase quantum cloning with input $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)$ can be realized by both economic and non-economic transformations with completely the same optimal fidelity. We suppose that qubit implemented by quantum device is precious, so we should prefer to economic phase cloning.

On the other hand, there exist some subtle differences between those two cases which are not generally noticed. For convenience, let us present explicitly those transformations. From the general results in Eq.(187), the optimal phase-covariant cloning transformation takes the form,

$$
\begin{aligned}
|0\rangle &\rightarrow \frac{1}{\sqrt{2}}|00\rangle|0\rangle_a + \frac{1}{2}\left(|01\rangle + |10\rangle\right)|1\rangle_a, \\
|1\rangle &\rightarrow \frac{1}{\sqrt{2}}|11\rangle|1\rangle_a + \frac{1}{2}\left(|01\rangle + |10\rangle\right)|0\rangle_a,
\end{aligned} \tag{190}
$$

where the subindex a denotes the ancillary state. With the help of Eq.(189), the economic phase-covariant cloning takes the following form, which is also presented in Eq.(169) and here we choose asymmetric parameter $\eta = \pi/4$,

$$
\begin{aligned}
|0\rangle &\rightarrow |0\rangle|0\rangle, \\
|1\rangle &\rightarrow \frac{1}{\sqrt{2}}(|1\rangle|0\rangle + |0\rangle|1\rangle),
\end{aligned} \tag{191}
$$

We already know that the fidelities of both economic and non-economic are the same and optimal, see Eq.(174),

$$
F_{optimal} = \frac{1}{2} + \sqrt{\frac{1}{8}}. \tag{192}
$$

The single qubit reduced density matrix of output from (190) can be calculated as,

$$
\rho_{red.} = \frac{1}{\sqrt{2}}|\psi\rangle\langle\psi| + \left(\frac{1}{2} - \sqrt{\frac{1}{8}}\right)\mathbb{I} = \begin{pmatrix} \frac{1}{2} & \frac{1}{\sqrt{8}}e^{-i\phi} \\ \frac{1}{\sqrt{8}}e^{i\phi} & \frac{1}{2} \end{pmatrix} \tag{193}
$$

It takes the scalar form, i.e., the single output can be written as a mixture of input qubit and a completely mixed state $\mathbb{I}/2$.

In comparison, the single qubit reduced density matrix of output from economic case is,

$$
\rho_{red.}^{eco.} = \begin{pmatrix} \frac{3}{4} & \frac{1}{\sqrt{8}}e^{-i\phi} \\ \frac{1}{\sqrt{8}}e^{i\phi} & \frac{1}{4} \end{pmatrix}. \tag{194}
$$

This form does not satisfy the scalar form. It also means relation $T(\mathbb{I}) = \mathbb{I}$ is not satisfied.

In eavesdropping of well known BB84 QKD, because all four states $|0\rangle, |1\rangle, 1/\sqrt{2}(|0\rangle + |1\rangle), 1/\sqrt{2}(|0\rangle - |1\rangle)$ can be described by $|\Psi\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$. So, instead of the UQCM, we should at least use the cloning machine for equatorial qubits in eavesdropping. Actually in individual attack, we can not do better than the cloning machine for equatorial qubits (Bruß *et al.*, 2000a). The cloning machine presented in equations (191,190) can be used in analyzing the eavesdropping of other two mutually unbiased bases $1/\sqrt{2}(|0\rangle - |1\rangle), 1/\sqrt{2}(|0\rangle + |1\rangle), 1/\sqrt{2}(|0\rangle + i|1\rangle), 1/\sqrt{2}(|0\rangle - i|1\rangle)$ which belong to $|\psi\rangle = (|0\rangle + e^{i\phi}|1\rangle)/\sqrt{2}$.

G. Phase-covariant quantum cloning for qudits

The phase quantum cloning can be applied to higher dimensional system. For qutrit case, the optimal fidelity was obtained by D'Ariano *et al.*(D'Ariano and Lo Presti, 2001) and Cerf *et al.*(Cerf *et al.*, 2002b);

$$F = \frac{5+\sqrt{17}}{12}, \quad \text{for } d=3. \tag{195}$$

In this review, we consider the general case in d-dimension (Fan *et al.*, 2003).

The input state is restricted to have the sample amplitude parameter but have arbitrary phases

$$|\psi\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} e^{i\phi_j}|j\rangle, \tag{196}$$

where phases $\phi_j \in [0, 2\pi), j = 0, \cdots, d-1$. A whole phase is not important, so we can assume $\phi_0 = 0$. For comparing the input and the single qudit output, here we write the density operator of input as $\rho^{(in)} = \frac{1}{d}\sum_{jk} e^{i(\phi_j - \phi_k)}|j\rangle\langle k|$. Our aim is to find the optimal quantum cloning transformations so that each output qudit is close to this input density operator.

Considering the symmetries, we can propose the following simple transformations,

$$U|j\rangle|Q\rangle = \alpha|jj\rangle|R_j\rangle + \frac{\beta}{\sqrt{2(d-1)}}\sum_{l\neq j}^{d-1}(|jl\rangle + |lj\rangle)|R_l\rangle, \tag{197}$$

where α, β are real numbers, and $\alpha^2+\beta^2 = 1$. Actually letting α, β to be complex numbers does not improve the fidelity. $|R_j\rangle$ are orthonormal ancillary states.

Substituting the input state (196) into the cloning transformation and tracing out the ancillary states, the output state takes the form

$$\begin{aligned} \rho^{(out)} &= \frac{\alpha^2}{d}\sum_j |jj\rangle\langle jj| + \frac{\alpha\beta}{d\sqrt{2(d-1)}}\sum_{j\neq l} e^{i(\phi_j-\phi_l)}\,[|jj\rangle(\langle jl| \\ &\quad +\langle |lj|) + (|jl\rangle + |lj\rangle)\langle ll|] \\ &+ \frac{\beta^2}{2d(d-1)}\sum_{jj'}\sum_{l\neq j,j'} e^{i(\phi_j-\phi_{j'})}(|jl\rangle + |lj\rangle)(\langle lj'| + \langle j'l|). \end{aligned} \tag{198}$$

Then, we can obtain the single qudit reduced density matrix of output

$$\begin{aligned} \rho^{(out)}_{red.} &= \frac{1}{d}\sum_j |j\rangle\langle j| \\ &\quad + \left(\frac{\alpha\beta}{d}\sqrt{\frac{2}{d-1}} + \frac{\beta^2(d-2)}{2d(d-1)}\right)\sum_{j\neq k} e^{i(\phi_j-\phi_k)}|j\rangle\langle k|. \end{aligned} \tag{199}$$

The fidelity can be calculated as

$$F = \frac{1}{d} + \alpha\beta\frac{\sqrt{2(d-1)}}{d} + \beta^2\frac{d-2}{2d}. \tag{200}$$

Now, we need to optimize the fidelity under the restriction $\alpha^2+\beta^2 = 1$. We can find the optimal fidelity of 1 to 2 phase-covariant quantum cloning machine can be written as

$$F_{optimal} = \frac{1}{d} + \frac{1}{4d}(d-2+\sqrt{d^2+4d-4}). \tag{201}$$

The optimal fidelity is achieved when α, β take the following values,

$$\begin{aligned} \alpha &= \left(\frac{1}{2} - \frac{d-2}{2\sqrt{d^2+4d-4}}\right)^{\frac{1}{2}}, \\ \beta &= \left(\frac{1}{2} + \frac{d-2}{2\sqrt{d^2+4d-4}}\right)^{\frac{1}{2}}. \end{aligned} \tag{202}$$

In case $d = 2, 3$, this results reduce to previous known results (174,195), respectively. As expected, this optimal fidelity of phase-covariant quantum cloning machine is higher than the corresponding optimal fidelity of UQCM,

$$F_{optimal} > F_{universal} = (d + 3)/2(d + 1). \tag{203}$$

These are the optimal phase-covariant quantum cloning machine for qudits (197, 202) and the optimal fidelity (201).

H. Symmetry condition and minimal sets in determining quantum cloning machines

In this subsection, we will mainly discuss how symmetry condition determines the form of quantum cloning machine. We will also consider the minimal sets in determining those quantum cloning machines.

As we shown, the number of BB84 states is four. The optimal cloning of those four states actually can clone optimally arbitrary corresponding equatorial qubits. This means that BB84 states are enough in determining the phase-covariant quantum cloning machine. We would come up with a question that whether they are the minimal input sets necessarily for the phase-covariant cloning. It is revealed that the set of BB84 states is not the minimal input set. The minimal set which determines the phase cloning machine is supposed to possess the highest symmetry in Bloch sphere with the number three. Here, we give a brief proof.

Consider three input states $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)$ where $\phi = 0, 2\pi/3, 4\pi/3$ which are finite numbers. We suppose that the quantum cloning machine works in symmetric subspace and is economic. The most general form can be written as,

$$\begin{aligned} |0\rangle &\to a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \\ |1\rangle &\to e|00\rangle + f|01\rangle + g|10\rangle + h|11\rangle, \end{aligned} \tag{204}$$

where a to h are complex numbers which satisfy constrains $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$,$|e|^2 + |f|^2 + |g|^2 + |h|^2 = 1$ and $ae^* + bf^* + cg^* + dh^* = 0$ due to orthogonal and normalizing conditions. Because the machine works in symmetric subspace, we have $b = c$ and $f = g$. It is easily calculated that the fidelity for arbitrary input equatorial state is,

$$F_A(\phi) = \frac{1}{2} + \frac{1}{2} Re[ac^* e^{(i\phi)} + ag^* + ec^* e^{(2i\phi)} + eg^* e^{(i\phi)} + bd^* e^{(i\phi)} + fh^* e^{(i\phi)} + fd^* e^{(2i\phi)} + bh^*]. \tag{205}$$

Simplify the expression by utilizing constrains above, we find

$$F_A(\phi) = \lambda_1 \cos(2\phi + \psi_1) + \lambda_2 \cos(\phi + \psi_2) + \lambda_3, \tag{206}$$

where $\lambda_i, i = 1, 2, 3$, are real numbers. Explicit expressions of these parameters are: $\lambda_1 = \frac{1}{2}|ec^* + fd^*|$, $\psi_1 = arg(ec^* + fd^*)$, $\psi_2 = \frac{1}{2}|ac^* + eg^* + bd^* + fh^*|$, $\psi_2 = arg(ac^* + eg^* + bd^* + fh^*)$, and $\lambda_3 = \frac{1}{2} + \frac{1}{2}Re(ag^* + bh^*)$.

Additionally, we let the cloning fidelities for those three states being the same: $F(0) = F(2\pi/3) = F(4\pi/3)$. We will obtain two more constraints: $\lambda_1 \sin\psi_1 = \lambda_2 \sin\psi_2$, $\lambda_1 \cos\psi_1 + \lambda_2 \cos\psi_2 = 0$. With the help of some algebraic inequalities, one would find that F reaches its maximum value if and only if $\lambda_1 = \lambda_2 = 0$. Now we are ready to find a simple form of the fidelity for the three input states,

$$F_A = \lambda_3. \tag{207}$$

Remarkably, this result demonstrates that for any ϕ, F_A is independent of the phase parameter ϕ. This cloning machine becomes the standard phase-covariant quantum cloning machine. Note that the minimal set include three states which is studied from the viewpoint of detection (Peres and Wootters, 1991).

Other similar results are also ready here:

1. For non-economic case, i.e., with the help of ancillary states, this conclusion remains correct.

2. For $1 \to M$ cases, this conclusion still remains correct.

As geometric symmetry only provides intuitive understanding in no more than three dimension, higher dimension cases may not be obvious. This might be explored further. Quantum cloning machine for 6-state protocol can be proved equivalent to UQCM which is discussed in the above section. It is similar to look for its corresponding determination sets by considering the symmetry, four states forming the tetrahedron with equivalent distance on Bloch sphere are the answer, see Fig.(3).

Since phase quantum cloning is corresponding to quantum phase estimation. The minimal input set may shed some light on the quantum state estimation. It is also interesting to study quantum cloning machine working between two fixed latitudes in the Bloch sphere. Contrary to phase-covariant quantum cloning machine, the mean fidelity in the region does not remain increasing from equator to polar, but has a minimum value.

I. Quantum cloning machines of arbitrary set of MUBs

Here, we discussed the higher dimension quantum cloning of the mutual unbiased basis(MUB). It is known that a Hilbert space of d dimension contains $d+1$ sets of MUB, provided d is prime. In this review, when MUBs are used, we will restrict our attentions on case d is prime. We can design QKD protocols by using arbitrary sets of MUBs. For example, in 2 dimensional system, we have two well accepted QKD protocols, six-state protocol means 3 sets of MUBs and BB84 protocol means 2 sets. In higher dimension, we can also propose corresponding cloning machines for those sets of MUBs.

Let us first present some characteristics of MUBs. In a system of dimension d, there are $d+1$ MUBs (Bandyopadhyay *et al.*, 2002), namely $\{|i\rangle\}$ and $\{|\tilde{i}^{(k)}\rangle\}$ $(k=0,1,...,d-1)$, are expressed as,

$$|\tilde{i}^{(k)}\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\omega^{i(d-j)-ks_j}|j\rangle, \tag{208}$$

with $s_j = j+...+(d-1)$ and $\omega = e^{i\frac{2\pi}{d}}$. Any states in the same set are orthogonal $\langle\tilde{i}^{(k)}|\tilde{l}^{(k)}\rangle = \delta_{il}$, and any states in different sets satisfying $|\langle\tilde{i}^{(k)}|\tilde{l}^{(j)}\rangle| = \frac{1}{\sqrt{d}}$, $k\neq j$, that is their overlaps are the same. Define the generalized Pauli matrices σ_x and σ_z as, $\sigma_|j\rangle = |j+1\rangle$ and $\sigma_z|j\rangle = \omega^j|j\rangle$. Note that, as usual, we omit module d in equations. Then there are d^2-1 independent Pauli matrices $U_{mn} = (\sigma_x)^m(\sigma_z)^n$ and $U_{mn}|j\rangle = \omega^{jn}|j+m\rangle$. Those MUBs are eigenvectors of operators $\sigma_z, \sigma_x(\sigma_z)^k$, $k=0,1,...,d-1$,

$$\sigma_x(\sigma_z)^k|\tilde{i}^{(k)}\rangle = \omega^i|\tilde{i}^{(k)}\rangle. \tag{209}$$

The result of MUBs can also be found in (Wootters and Fields, 1989).

A straightforward generalization of BB84 states in d-dimension is two sets of bases from those $d+1$ MUBs, and the generalization of six-state protocol is to use all $d+1$ mutually unbiased bases (Cerf *et al.*, 2002a). Suppose two MUBs are $\{|k\rangle\}, k=0,1,2,...,d-1$ and its dual under a Fourier transformation,

$$|\bar{l}\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}e^{2\pi i(kl/d)}|k\rangle, \tag{210}$$

where l=0,1,2,...,d-1. We follow the standard QKD, Alice initially sends the state $|\psi\rangle$, Eve can use her quantum clone machine to copy the state and the transferring state is disturbed which is later still sent to Bob. Eve has a non-perfect copy of the sending state and the ancillary state of her quantum cloning machine. The whole system is written as,

$$|\psi\rangle_A \rightarrow \sum_{m,n=0}^{d-1} a_{m,n}U_{m,n}|\psi\rangle_B|B_{m,-n}\rangle_{E,E'}, \tag{211}$$

where A,B,E, and E' represent Alice's qudit, Bob's clone, Eve's clone, and the cloning machine. Obviously, parameters $a_{m,n}$ satisfy $\sum_{m,n=0}^{d-1}|a_{m,n}|^2 = 1$. As we already know, $|B_{m,-n}\rangle_{EE'}$ stands for d-dimensional Bell states which is the maximally entangled states of two qubits with explicit form:

$$|B_{m,n}\rangle_{EE'} = \frac{1}{\sqrt{d}}\sum_{k=0}^{N-1}e^{2\pi i(kn/d)}|k\rangle_E|k+m\rangle_{E'}, \tag{212}$$

where $m,n = 0,1,...,d-1$. Note that the operators $U_{m,n}$ can be expressed as,

$$U_{m,n} = \sum_{k=0}^{d-1}e^{2\pi i(kn/d)}|k+m\rangle\langle k|. \tag{213}$$

They actually form a group of qudit error operations where m represents the shift errors and n is related with the phase errors. Trace off the joint states within Eve, Bob's clone will be a mixed state, it is the same as the state $|\psi\rangle$ passing through a quantum channel which will cause decoherence,

$$\rho_B = \sum_{m,n=0}^{d-1}|a_{m,n}|^2U_{m,n}|\psi\rangle\langle\psi|U_{m,n}^\dagger. \tag{214}$$

Therefore, when Alice sends states $|k\rangle$, Bob's fidelity is

$$F = \langle k|\rho_B|k\rangle = \sum_{n=0}^{d-1} |a_{0,n}|^2. \tag{215}$$

Also, when Alice sends states $|\bar{l}\rangle$, Bob's fidelity is

$$\bar{F} = \langle \bar{l}|\rho_b|\bar{l}\rangle = \sum_{m=0}^{d-1} |a_{m,0}|^2. \tag{216}$$

Consider the requirement that the cloner works equally well with these states, we must choose the amplitude matrix as the following form,

$$a = \begin{pmatrix} v & x & \cdots & x \\ x & y & \cdots & y \\ \vdots & \vdots & \ddots & \vdots \\ x & y & \cdots & y \end{pmatrix} \tag{217}$$

where x, y and v are real number satisfying $v^2 + 2(d-1)x^2 + (d-1)^2y^2 = 1$. In this way, we find Bob's fidelity is

$$F = v^2 + (d-1)x^2. \tag{218}$$

Further, we find that the fidelity for Eve can be expressed as,

$$F_E = v'^2 + (d-1)x'^2 \tag{219}$$

where v', x' and y' come from the Fourier transformation,

$$b_{m,n} = \frac{1}{d}\sum_{m',n'=0}^{d-1} e^{2\pi i(nm'-mn')/d} a_{m',n'}. \tag{220}$$

The explicit form can be written as,

$$\begin{aligned} x' &= [v + (d-2)x + (1-d)y]/d, \\ y' &= (v - 2x + y)/d, \\ v' &= [v + 2(d-1)x + (d-1)^2y]/d. \end{aligned} \tag{221}$$

Note that b_{mn} comes from the following expression,

$$U = \sum_{m,n=0}^{d-1} a_{mn}(U_{mn} \otimes U_{m,-n} \times \mathbb{I}) \tag{222}$$

Our purpose is to maximize Eve's fidelity F_E under a given value of Bob's fidelity F. The trade-off relation can be found as,

$$F_E = \frac{F}{d} + \frac{(d-1)(1-F)}{d} + \frac{2}{d}\sqrt{(d-1)F(1-F)}. \tag{223}$$

Next, we consider another protocol using all available $d+1$ bases. Similarly, by considering that the same fidelity is necessary for all used bases since they are applied randomly, we derive that amplitude matrix presented in Eq.(217) must satisfy $x = y$. Hence, Bob's fidelity is

$$F = v^2 + (d-1)x^2 = 1 - d(d-1)x^2, \tag{224}$$

and Eve's fidelity is,

$$F_E = v'^2 + (d-1)x'^2 = 1 - d(d-1)x'^2, \tag{225}$$

where v' and x' are expressed as

$$\begin{aligned} x' &= (v-x)/d \\ v' &= [v+(d^2-1)x]/d. \end{aligned} \tag{226}$$

The relations induce the trade-off between two fidelities of Bob and Eve.

For higher dimension case, we may have more choices for QKD. Besides by using only two bases or all $d+1$ bases, we may choose any sets of mutually unbiased bases. Then corresponding cloning machines are necessary in analyzing the security. Those general QKD protocols are studied recently in (Xiong *et al.*, 2012). By using the same arguments about the symmetry, we can find,

$$\rho_B = \sum_{m,n=1}^{d-1} |a_{mn}|^2 |i+m\rangle\langle i+m|, \tag{227}$$

$$\tilde{\rho}_B^{(k)} = \sum_{m,n=0}^{d-1} |a_{mn}|^2 (U_{mn}|\tilde{i}^{(k)}\rangle_B)({}_B\langle\tilde{i}^{(k)}U_{mn}^\dagger), \tag{228}$$

$$\rho_E = \sum_{m,n=1}^{d-1} |b_{mn}|^2 |i+m\rangle\langle i+m|, \tag{229}$$

$$\tilde{\rho}_E^{(k)} = \sum_{m,n=0}^{d-1} |b_{mn}|^2 (U_{mn}|\tilde{i}^{(k)}\rangle_E)({}_E\langle\tilde{i}^{(k)}U_{mn}^\dagger), \tag{230}$$

where $k=0,1,...,g-1$. Therefore, one may easily derive the fidelities,

$$F_B = \sum_n |a_{0n}|^2, \tag{231}$$

$$\tilde{F}_B^{(k)} = \sum_m |a_{m,km}|^2, \tag{232}$$

$$F_E = \frac{1}{d}\sum_m |\sum_n a_{mn}|^2, \tag{233}$$

$$\tilde{F}_E^{(k)} = \frac{1}{d}\sum_n |\sum_m a_{m,n+km}|^2, \tag{234}$$

$$\tag{235}$$

where $k=0,1,...,g-1$. Assuming that Eve's attack is balanced, or we say she induces an equal probability of error for any one of the $g+1$ MUBs, we have,

$$F_B = \tilde{F}_B^{(0)} = ... = \tilde{F}_B^{(g-1)}. \tag{236}$$

These constraints can determine the optimal cloner. Eve could maximize all these $g+1$ fidelities simultaneously and and let them equal. This is can be realized by "vectorization" of the matrix elements of (a_{mn}). Define,

$$\vec{\alpha}_i = (a_{1,1i},...,a_{d-1,(d-1)i}), \quad (i=0,1,...,g-1), \tag{237}$$

$$\vec{A}_i = (A_1,...,A_{d-1}), \tag{238}$$

$$A_i = \sum_{j\neq 0,i,...,(g-1)i}^{d-1} a_{ij} (i=1,2,...,d-1), \tag{239}$$

and the rest elements are restricted by the following equations:

$$\sum_{j=1}^{d-1} |a_{0j}|^2 = F_B - |a_{00}|^2, \tag{240}$$

$$||\vec{\alpha}_i||^2 = F_B - |a_{00}|^2, \quad (i=0,1,...,g-1). \tag{241}$$

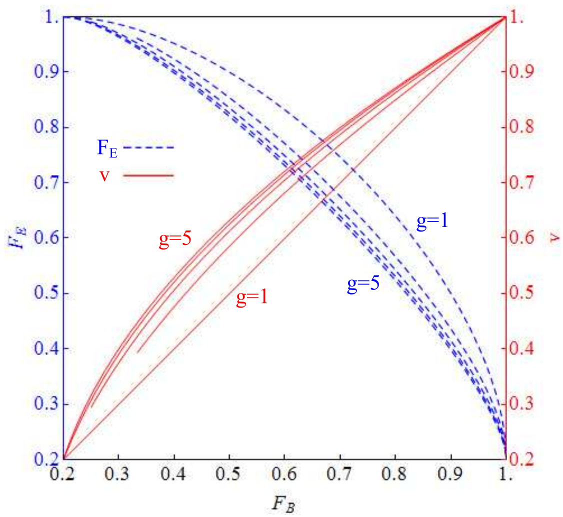


FIG. 5 The fidelities of Bob and Eve for dimension $d = 5$. The number of mutually unbiased bases runs from 2 to 6. These results are presented in (Xiong *et al.*, 2012).

Finally, Eve's fidelity can be expressed as

$$F_E = \frac{1}{d}(|\sum_{j=0}^{d-1} a_{0j}|^2 + ||\sum_{i=0}^{g-1} \vec{\alpha}_i + \vec{A}||^2). \tag{242}$$

By maximizing Eve's fidelity, the above result can be further simplified by some algebraic considerations,

$$a_{mn} = \begin{cases} v, \ m = n = 0, \\ x, \ m = 0, n \neq 0 \text{ or } m \neq 0, n = km, \\ y, \ \text{ otherwise}, \end{cases} \tag{243}$$

where $k = 0, ..., g-1$, and v is a real number to be determined and $x = \sqrt{\frac{F_B - v^2}{d-1}}$, $y = \sqrt{\frac{1+gv^2-(g+1)F_B}{(d-1)(d-g)}}$. Now we reach our conclusion that the fidelity of Eve is,

$$F_E = \frac{1}{d}\{[v + (d-1)x]^2 + (d-1)[gx + (d-g)y]^2\}. \tag{244}$$

The only undetermined variable is v, we can change it so that the fidelity of Eve F_E reaches the maximum depending on the fixed fidelity of Bob. The fidelities of Bob and Eve are presented in FIG.5 for some special cases (Xiong *et al.*, 2012).

From this conclusion, we may easily find out the results for $g = 1$ and $g = d$ which lead to results in (Cerf *et al.*, 2002a). Also we are interested in the condition that $F_B = F_E$ which is the symmetric cloning, and the remained variable v is fixed in this case which actually takes a rather complicated form, we finally have,

$$F = \frac{2}{d}\frac{d-g}{(g+3) - \sqrt{(g+3)^2 - 8\frac{(d-g)(g+1)}{d}}}. \tag{245}$$

As we know, the optimal cloner for $d+1$ MUBs is actually equivalent to universal quantum cloning machine. It is interesting to know which of the above quantum cloning machine is equivalent to the phase-covariant quantum cloning machine. Stimulated by the fact that d MUBs presented in Eq.(208) only contain phase parameters but the amplitude parameters are fixed, we may suppose that the d-dimension phase-covariant quantum cloning should be equal to the cloning of d MUBs. Indeed, let $g = d-1$, the fidelity (245) coincides with the phase-covariant fidelity in (201). To further check that those two cloning machines are the same, we need also consider the asymmetric case.

Let us consider the equatorial qudit as, $|\psi\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} e^{i\phi_j}|j\rangle$, where ϕ_j are phase parameters. One can assume that the asymmetric cloning transformation is given as,

$$|i\rangle \to \alpha|ii\rangle|i\rangle + \frac{\beta}{\sqrt{d-1}}\sum_{j\neq i}(\cos\theta|ij\rangle + \sin\theta|ji\rangle|j\rangle), \tag{246}$$

where θ is the asymmetric parameter. Therefore one can derive two fidelities for Bob and Eve, respectively,

$$F_1 = \frac{1}{d} + \frac{2\alpha\beta}{d}\sqrt{d-1}\cos\theta + \frac{\beta^2(d-2)}{d}\cos^2\theta, \tag{247}$$

$$F_2 = \frac{1}{d} + \frac{2\alpha\beta}{d}\sqrt{d-1}\sin\theta + \frac{\beta^2(d-2)}{d}\sin^2\theta, \tag{248}$$

where we still have $\alpha^2 + \beta^2 = 1$. Here we would like to emphasize, the exact value of α, β should depend on the parameter θ. For symmetric case, $\theta = \pi/4$, their values can be found in Eqs.(202). When θ changes, the values of α, β also change. Numerical evidences show that those fidelities are the same with the fidelities in Eq.(244).

J. Other developments and related topics

In a short summary for this subsection, we have known that UQCM and phase-covariant cloning machine are just special cloners for some sets of MUBs. We remark that the quantum cloning of sets of MUBs should be related with states estimation. The results of arbitrary state estimation and phase estimation are available which correspond to $g = d, d-1$, however, the general $g+1$ MUBs estimations are not yet studied. For higher-dimension case, the cloning of states with only real parameters is studied in (Navez and Cerf, 2003). The asymmetric qudit phase-covariant quantum cloning is studied in (Lamoureux and Cerf, 2005). The quantum cloning of set of states which is invariant under the Weyl-Heisenberg group is studied by the extremal cloning machine (Chiribella *et al.*, 2005). The phase estimation of qubits is studied in (Derka *et al.*, 1998), the case of qubits in mixed states is presented in (D'Ariano *et al.*, 2005a). The phase estimation of multiple phases is studied in (Macchiavello, 2003). The QKD in three dimension is studied in (Bruß and Macchiavello, 2002). The four-dimensional case is studied in (Bechmann-Pasquinucci and Tittel, 2000; Durt and Nagler, 2003), The optimal eavesdropping of BB84 states is studied in (Fuchs *et al.*, 1997), higher-dimensional case and some related results are presented by some other groups (Acín *et al.*, 2003; Bae and Acin, 2007; Bourennane *et al.*, 2001; Karimipour *et al.*, 2002; Kraus *et al.*, 2005; Nikolopoulos and Alber, 2005; Nikolopoulos *et al.*, 2006). The extension of BB84 states for qubits is also studied as the spherical-code (Renes, 2004). The comparison between photon-number-splitting attack and quantum cloning attack of BB84 states is studied in (Niederberger *et al.*, 2005). The extension of phase-covariant cloning to multipartite quantum key distribution is studied in (Scarani and Gisin, 2001). We should note that the security of QKD is generally defined by various criteria (Gisin *et al.*, 2002), in this review, we consider the attack by the scheme of quantum cloning. Quantum copying of two states is studied in (Hillery and Bužek, 1997). The cloning of a pair of orthogonally polarized photons is studied in (Fiurasek and Cerf, 2008). The quantum cloning of states with fixed amplitudes but arbitrary phase is studied in (Karimipour and Rezakhani, 2002), which is suboptimal while the experimental scheme uses the optimal one (Du *et al.*, 2005). The cloning of states in a belt of Bloch sphere is studied in (Hu *et al.*, 2009). The case of distribution with mirror like symmetry, i.e., with known modulus of expectation of Pauli σ_z matrix is studied in (Bartkiewicz *et al.*, 2009), the case of arbitrary axisymmetric distribution on the Bloch sphere is studied in (Bartkiewicz and Miranowicz, 2010), see also (Bartkiewicz and Miranowicz, 2012). The economic realization of phase-covariant devices in arbitrary dimension, where phase cloning as a special case, is studied in (Buscemi *et al.*, 2007). The scheme of one to three economic phase-covariant quantum cloning machine is proposed to be implemented by linear optics system (Zou and Mathis, 2005). The one to many symmetric economic phase cloning is proposed in (Zhang *et al.*, 2007), see also (Zhang and Ye, 2009). The scheme to realize economic one to many phase cloning for qubit and qutrit is proposed in (Zou *et al.*, 2006). The assisted phase cloning of qudit by remote state preparation is presented in (Ma and Zhan, 2009). The network of state-dependent quantum cloning is studied in (Chefles and Barnett, 1999), see also (Zhou, 2011). The realization of phase-covariant and real qubit state quantum cloning are presented in (Fang and Ye, 2010). The phase cloning in spin networks is proposed in (Chiara *et al.*, 2004). The relations between teleportation between dissipative channels with the universal and phase-covariant cloning machine are analyzed in (Ozdemir *et al.*, 2007). The criterion for estimation the quality of state-dependent cloning is analyzed in (Rastegin, 2002). The proposal of optical implementation of phase cloning of qubits is presented in (Fiurášek, 2003), the cloning of real state is studied in (Hu *et al.*, 2010). The one to many phase-covariant quantum cloning is also analyzed by the general angular momentum formalism (Sciarrino and De Martini, 2007).

Experimentally, the asymmetric phase cloning is realized in optical system (Bartuskova *et al.*, 2007), and in (Soubusta *et al.*, 2008). The ancilla-free phase-covariant cloning realized by Hong-Ou-Mandel interference is realized in experiment by Khan and Howell (Khan and Howell, 2003). The one to three economic quantum cloning of equatorial qubits encoded by polarization states of photons and the universal cloning are realized experimentally in (Xu *et al.*, 2008). NMR system (Chen *et al.*, 2007; Du *et al.*, 2005). In optical parametric amplification of a single photon in the high gain-regime, experiment is performed to distribute the photon polarization state to a large number of particles which corresponds to the phase-covariant quantum cloning (Nagali *et al.*, 2007). The phase-covariant

quantum cloning is implemented in nitrogen-vacancy center of diamond by using three energy levels (Pan *et al.*, 2011). The experimental implementation of eavesdropping of BB84 states and trine states by optimal cloning is studied in (Bartkiewicz *et al.*, 2012).

Quantum cloning is generally not concerned with relativity, with relativistic covariance requirement, the state-dependent cloning of photons and the BB84 states are studied in (Bradler and Jauregui, 2008). It is shown by phase-covariant quantum cloning that the cloned quantum states are not macroscopic in the spirit of Schrodinger's cat (Frowis and Dür, 2012). The cloning network of generalized BB84 states constituted by two pairs of orthogonal states is presented in (Cao and Song, 2004). The state-dependent cloning machine and the relation with completely positive trace-preserving maps is studied in (Carlini and Sasaki, 2003). The phenomena of superbroadcasting is also studied for phase-covariant case (Buscemi *et al.*, 2006). The optimal broadcasting of mixed equatorial qubits is studied in (Yu, 2009). Quantum circuits for both entanglement manipulation and asymmetric phase-covariant cloning are studied in (Levente *et al.*, 2010). Relation of state-dependent cloning with quantum tracking is studied in (Mendonca *et al.*, 2008). The no-cloning theorem for a single POVM is presented in (Rastegin, 2010). A hybrid quantum cloning machine combines universal and state-dependent cases together is presented in (Adhikari *et al.*, 2007). While equatorial qubit contains only one arbitrary parameter, the phase information cannot be compressed (Wang *et al.*, 2012).

VI. LOCAL CLONING OF ENTANGLED STATES, ENTANGLEMENT IN QUANTUM CLONING

Quantum cloning is generally to find the quantum operations to realize the optimal cloning. The only restriction is that the operations should satisfy quantum mechanics. We next study the local cloning of entangled states, in this case, the operations are additionally restricted to be local. In principle, there is also a no-cloning theorem for entangled states (Koashi and Imoto, 1998).

In addition, since the crucial role of quantum entanglement in quantum information, we will also study the entanglement properties in quantum cloning machines.

A. Local cloning of Bell states

Quantum entanglement plays a key role in quantum computation and quantum information. It is the precious resource in quantum information processing. Also entanglement is a unique property of quantum system which does not have any classical correspondence. In this sense, quantum entanglement has already become a common concept and has many applications in various quantum systems. The study of entanglement is generally under the condition of local (quantum) operations and classical communication (LOCC). This is due to the consideration that entanglement does not increase under LOCC.

The local cloning of entangled states is an interesting topic (Anselmi *et al.*, 2004; Bužek *et al.*, 1997b; Ghosh *et al.*, 2004; Owari and Hayashi, 2006). First let us raise the problem: Suppose two spatially separated parties, Alice (A) and Bob (B), share some entangled states, by LOCC, they want to copy the shared entangled states. As an example, let us study the following problem (Ghosh *et al.*, 2004), the four Bell states are defined as usual as the following,

$$
\begin{aligned}
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = (I \otimes Z)|\Phi^+\rangle, \\
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = (I \otimes X)|\Phi^+\rangle, \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). = (I \otimes XZ)|\Phi^+\rangle. \qquad (249)
\end{aligned}
$$

Alice and Bob share one Bell states from a known subset, say $\{|\Psi^+\rangle, |\Phi^+\rangle\}$, they want to copy this state by LOCC. Several problems should be considered before to study this problem: (1).The entanglement between A and B does not increase under LOCC. So to copy locally this state, we generally assume that some known entangled states, for example $|\Phi^+\rangle$, are shared between A and B which can be used as ancilla. (2).The entanglement resource used by local copying should be minimum. Otherwise, we can use the teleportation scheme(Bennett *et al.*, 1993), let Bob (Alice) obtain the full state $\{|\Psi^+\rangle, |\Phi^+\rangle\}$, he knows the state exactly by measurement, and copies of the entangled state between A and B can be obtained easily by local unitary operations which are shown explicitly above in (249). Actually Alice and Bob can discriminate any two Bell states by LOCC (Ghosh *et al.*, 2001; Walgate and Hardy, 2002; Walgate *et al.*, 2000).

In these conditions, the problem can be explicitly stated as: Alice and Bob share either of two maximally entangled states $\{|\Psi^+\rangle, |\Phi^+\rangle\}$ and an ancilla $|\Phi^+\rangle$, can they obtain the state $|\Psi^+\rangle^{\otimes 2}$ or $|\Phi^+\rangle^{\otimes 2}$ by LOCC? The answer is 'yes': both Alice and Bob do CNOT gate with the unknown qubit as the controlled qubit and the ancilla as the target qubit, they can achieve their aim. We name this method as CNOT scheme. The key point here is that Alice and Bob do not need to know which state they share, they can finally obtain two copies of this state, and only one known state $|\Phi^+\rangle$ (resource) is consumed. Let us next analyze the advantages of this scheme. If we use the teleportation, then discriminate the state, finally prepare the two copies, we find that three Bell states $|\Phi^+\rangle$ (resource) are used. If we use the local discrimination, i.e. by local measurement in $\{|0\rangle, |1\rangle\}$ basis and with assistance of classical communication, we know the exact form of the shared state, the two copies can be obtained by local unitary operations. In this scheme, two Bell sates are consumed. On the other hand, to obtain two copies of $|\Psi^+\rangle$ or $|\Phi^+\rangle$, at least, one ancilla should be used. So the CNOT scheme is optimal.

B. Local cloning and local discrimination

If a set of quantum states can be perfected discriminated, they can be copied perfectly since we can discriminate them first, then prepare many copies of these states by using the available entanglement resource. For example, two

orthogonal states can be copied perfectly. We know that two Bell states can be locally discriminated, as shown in the last subsection, they can be local cloned perfectly if a *priori* Bell state resource is available. Is it generally true that local discrimination means local cloning being possible? In (Owari and Hayashi, 2006), it is stated that, in general, the local copying is more difficult than local discrimination.

However, local cloning and local discrimination are closely related (Owari and Hayashi, 2006). The following result was obtained in (Owari and Hayashi, 2006): For d-dimensional system, and suppose d is prime, a set of maximally entangled states $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ are defined as

$$|\Psi_j\rangle = (U_j \otimes I)|\Phi^+\rangle, \tag{250}$$

and

$$U_j = \sum_{j=0}^{D-1} \omega^{jk}|k\rangle\langle k|, \tag{251}$$

then the set $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ can be locally copied.

Here let us point out that the states of this set can be local discriminated perfectly according to the criteria proposed in (Fan, 2004). The scheme can be like the following. It is known that $U_j = \sigma_z^j$, where the generalized Pauli matrix $\sigma_z|k\rangle = \omega^k|k\rangle$. We define a class generalized Hadamard transformations as, up to an unimportant factor,

$$(H_\alpha)_{jk} = \omega^{-jk}\omega^{-\alpha s_k}, \tag{252}$$

where $s_k = k + ... + (d-1)$. We remark that those transformations correspond to the $d+1$ mutually unbiased states. By applying those Hadamard transformations, the generalized Pauli matrices transform as,

$$H_\alpha \sigma_x^m \sigma_z^n H_\alpha^\dagger = \sigma_x^{m\alpha+n}\sigma_z^{-m}. \tag{253}$$

Now we know that σ_z matrix can be transformed to σ_x matrix, $U_j \to \sigma_x^j$. Since $(\sigma_x^j \otimes I)\sum|kk\rangle = \sum|k+j,k\rangle$, that means those states can be distinguished by LOCC, also the above transformations correspond to local unitary operations, we now conclude that states in set $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ can be distinguished by LOCC.

We next see how those states can be cloned locally, define generalized CNOT gate as,

$$CNOT : |a\rangle|b\rangle \to |a\rangle|b+a\rangle, \tag{254}$$

where $|a+b\rangle$ modula d is assumed. We suppose an ancilla state $|\Phi^+\rangle$ is shared between Alice and Bob. Let both Alice and Bob perform the generalized CNOT gate, we obtain the perfect copies $|\Psi_j\rangle^{\otimes 2}$. This result can be derived as follows, according the definition of the CNOT gate, we know that

$$CNOT^\dagger : |a\rangle|b\rangle \to |a\rangle|b-a\rangle, \tag{255}$$

It is straightforward to check that we have the following properties

$$\begin{aligned} |\Phi^+\rangle_{12}|\Phi^+\rangle_{34} &= CNOT_{13}^\dagger \otimes CNOT_{24}^\dagger|\Phi^+\rangle_{12}|\Phi^+\rangle_{34} \\ &= CNOT_{13} \otimes CNOT_{24}|\Phi^+\rangle_{12}|\Phi^+\rangle_{34}. \end{aligned} \tag{256}$$

Then we can find

$$\begin{aligned} CNOT_{13} \otimes CNOT_{24}|\Psi_j\rangle_{12}|\Phi^+\rangle_{34}. &= CNOT_{13} \otimes CNOT_{24}(U_j \otimes I)_{13}|\Phi^+\rangle_{12}|\Phi^+\rangle_{34} \\ &= CNOT_{13}(U_j \otimes I)_{13}CNOT_{13}^\dagger|\Phi^+\rangle_{12}|\Phi^+\rangle_{34}. \end{aligned} \tag{257}$$

And we know the following result:

$$CNOT(U_j \otimes I)CNOT^\dagger = U_j \otimes U_j. \tag{258}$$

The operator U_j is copied. Thus by this method, a set of maximally entangled states $\{|\Psi_j\rangle\}_{j=0}^{N-1}$ are locally copied. This interesting phenomenon means that some unitary operators can be cloned perfectly in the above framework.

In 2-dimensional system, we have presented relations (45) for CNOT gate previously (Gottesman, 1998), $(\sigma_x \otimes I) \to \sigma_x \otimes \sigma_x, (\sigma_z \otimes I) \to \sigma_z \otimes I, (I \otimes \sigma_x) \to I \otimes \sigma_x, (I \otimes \sigma_z) \to \sigma_z \otimes \sigma_z$. Those results imply that the bit flip errors are copied forwards while the phase errors are copied backwards. But we cannot copy simultaneously the bit flip errors and phase flip errors. This is a kind of no-cloning theorem.

The local cloning of product states without the shared entanglement ancilla is studied in (Ji *et al.*, 2005). Distinguishing states locally is also studied in (Chen and Yang, 2001a,b; Walgate and Hardy, 2002; Walgate *et al.*, 2000). The local cloning of other cases are also studied, including three-qubit case (Adhikari and Choudhury, 2006), the continuous-variable case (Adhikari *et al.*, 2008), orthogonal entangled states and catalytic copying (Anselmi *et al.*, 2004). The local cloning of partially entangled pure states in higher dimension is studied in (Li and Shen, 2009). Some results of local cloning with entanglement resource are presented in (Chefles *et al.*, 2001; Collins *et al.*, 2001; Eisert *et al.*, 2000).

Various schemes of quantum cloning of entanglement are studied in (Karpov *et al.*, 2005; Lamoureux *et al.*, 2004). Quantum cloning of continuous-variable entangled states is studied in (Weedbrook *et al.*, 2008). The cloning of entangled photons to large scales which might be see by human eye is analyzed in (Sekatski *et al.*, 2010). The scheme of cloning unknown entangled state and its orthogonal-complement state with some assistances is studied in (Ma *et al.*, 2009) and also in (Zhan, 2005) and (Fang *et al.*, 2006), the case of arbitrary unknown two-qubit entangled state is studied in (Niu, 2009). The partial quantum cloning of bipartite state, i.e., only part of the of the two-particle state is cloned, and the cloning of mixed states are studied in (Kazakov, 2010). Coherent states cloning and local cloning are presented in (Dong *et al.*, 2008). The disentanglement is to preserve the local properties of an entangled state but erase the entanglement between the subsystems, it is closely related with quantum cloning and the broadcasting (Mor and Terno, 1999). The cloning machine used as approximate disentanglement is presented in (Yu *et al.*, 2004). The two-qubit disentanglement and inseparability correlation are presented in (Zhou and Guo, 2000).

C. Entanglement of quantum cloning

It is also of interest to know the entanglement structure of states in the quantum cloning machines. Potentially, those properties can be used to distinguish quantum from classical since entanglement is considered to be one unique property of quantum world.

There are much progress about the theory of entanglement, see (Horodecki *et al.*, 2009) for a nice review. For example, Peres-Horodeckis criteria (Horodecki *et al.*, 1996; Peres, 1996b) is simple to detect the entangled state. Since the output states of the quantum cloning machines are generally available, we can use various techniques to study the entanglement properties of the sole copies, or the whole output state of the cloning machine, or the copies with the ancillary states, etc.

In (Fan *et al.*, 2001b), it is shown that for the $1 \to 2$ cloning machines, the two copies of the UQCM are entangled, while the two copies for the phase-covariant cloning machine are separable. Further, we can use some measures of entanglement to quantify the entanglement. The entanglement structure or separability of the asymmetric phase-covariant quantum cloning is studied in (Rezakhani *et al.*, 2005). The bipartite and tripartite entanglement of the output state of cloning are studied in (Bruß and Macchiavello, 2003).

VII. TELECLONING

Quantum telecloning, as its name suggests, combines teleportation and quantum cloning so that quantum states are distributed to some more spatially separated parties. In the well-known teleportation scheme in (Bennett *et al.*, 1993), quantum information of an unknown d-level system is completely transmitted from a sender Alice to a remote receiver Bob by using the resource of a maximally entangled state. It is natural to consider "one-to-many" and "many-to-many" communication via quantum channels. This is the generalized teleportation scheme discussed in (Ghiu, 2003; Murao *et al.*, 2000). Of course, it is impossible to transmit quantum information with perfect fidelities for many copies, because the no-cloning theorem (Wootters and Zurek, 1982) claims that an unknown quantum state can not be cloned perfectly. However, as we already shown, we can try to quantum clone those quantum states approximately or probabilistically which are allowed by quantum mechanics.

As we already presented, there are various quantum cloning machines which create optimal copies. The aim of teleclone is to create optimal copies which is the same as that of the cloning machines, in addition, we need to create optimal copies remotely by teleportation. Those remote copies themselves may be spatially separated with each other. One may imagine that we can use first quantum cloning machines to create optimal copies locally, then send those copies to their destination points. The aim of teleclone can indeed be realized by this way. In this point, the importance of teleclone is like teleportation. Instead of teleportation, we can surely use flying qubits for states transportation. However, teleportation in the one hand provides an alternative method. On the other hand, in case the quantum channel is noisy, the flying qubits may experience inevitable decoherence which will induce errors. The teleportation scheme can avoid this disadvantage by using the maximally entangled state resource. Even when the entanglement resource is not perfect, the non-maximally entangled states can be purified locally to create maximally entangled states. Now we are ready to study teleclone which combines together the quantum cloning and the quantum teleportation. Still the resource of entanglement is necessary, however, its exact form depends on our specially designed scheme.

Murao *et al.* study the optimal telecloning of 1 qubit to M qubits by using maximally entangled state (Murao *et al.*, 1999). Telecloning which transmites an unknown d-level state to M spatially separated receivers is studied in (Murao *et al.*, 2000). And the telecloning of N qubits to M qubits, $M > N$, that requires positive valued operator measure (POVM) was proposed in (Dür and Cirac, 2000). These telecloning are also called reversible telecloning because there is no loss of quantum information. The $1 \to 2$ telecloning which uses nonmaximum entanglement (it is named irreversible telecloning, in comparison), is studied in (Bruß *et al.*, 1998a), and the generalized case, $1 \to M$ irreversible telecloning, is given in (Dür, 2001). Quantum information can be encoded by states of continuous variables (CV)(Braunstein and van Loock, 2005). The teleportation of CV is presented in (van Loock and Braunstein, 2000). The optimal 1 to M telecloning of CV coherent states using a $(M+1)$-partite entangled state as a multiuser quantum channel is shown in (van Loock and Braunstein, 2001). This optimal telecloning could be achieved by exploiting nonmaximum entanglement between the sender and receivers. So this protocol was regarded as a CV irreversible telecloning. A scheme of CV reversible $N \to M + (M - N)$ telecloning, which distributes information without loss, is presented in (Zhang *et al.*, 2006).

A. Teleportation

Let us review the original teleportation protocol and its generalization, i.e., the many-to-many scheme for transmitting quantum information. The teleportation scheme is proposed in (Bennett *et al.*, 1993). Alice wants to send an unknown state of a d-level particle to a spatially separated observer Bob with the help of quantum channel and classical communication. Alice's initial unknown state is,

$$|\psi\rangle = \sum_{k=0}^{d-1} \alpha_k |k\rangle_A, \tag{259}$$

where $\sum_{k=0}^{d-1} |\alpha_k|^2 = 1$ and $\{|k\rangle\}$ is a complete orthogonal basis. In order to achieve the teleportation, Alice and Bob are assumed to share a prior maximally entangled state, $|\xi\rangle = |\Phi^+\rangle$,

$$|\xi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_P |j\rangle_B. \tag{260}$$

The total system is, $|\Psi\rangle = |\psi\rangle \otimes |\xi\rangle$, which can be rewritten as,

$$|\Psi\rangle = |\psi\rangle_A \otimes |\xi\rangle_{PB} = \frac{1}{d}\sum_{m,n=0}^{d-1} |\Phi_{mn}\rangle_{AP} \sum_{k=0}^{d-1} \exp\Big(-i\frac{2\pi nk}{d}\Big)\alpha_k |k+m\rangle_B, \tag{261}$$

where $k+m$ is assumed to module d. As standard, the generalized Bell basis are,

$$|\Phi_{mn}\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1} \exp\Big(i\frac{2\pi nk}{d}\Big)|k\rangle|k+m\rangle. \tag{262}$$

Alice performs a joint Bell-type measurement on the input and port particles, sends the measurement result m, n to receiver Bob via classical communication. The unitary transformation which brings Bob's particle to the original state of Alice's is

$$U_{mn} = \sum_{j=0}^{d-1} exp\Big(i\frac{2\pi jn}{d}\Big)|j\rangle\langle j+m|. \tag{263}$$

As we already know, they are the generalized Pauli matrices in d dimension.

Next, we will review the generalized symmetric teleportation scheme of N senders and $M, (M > N)$, receivers proposed in (Ghiu, 2003). Assuming the senders $X_1, X_2, \cdots, X_N$ share an unknown, but with fixed form of entangled state $|\psi\rangle_X = \sum_{k=0}^{d-1} \alpha_k |\psi_k\rangle_{X_1}|\psi_k\rangle_{X_2}\cdots|\psi_k\rangle_{X_N}$, where $\{|\psi_k\rangle\}$ is an orthonormal basis of d-dimensional space. The quantum entangled state, consisting of N "port" particles $P_k(k = 1, \cdots, N)$ and M receivers $C_k(k = 1, \cdots, M)$, takes a special form which is a $(N + M)$-partite state,

$$|\xi\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} |\pi_j\rangle_{P_1}|\pi_j\rangle_{P_2}\cdots|\pi_j\rangle_{P_N}|\phi_j\rangle_{C_1C_2\cdots C_M}, \tag{264}$$

where $\{|\pi_j\rangle\}$ denotes a d-dimensional orthonormal basis. The complete state of the system is,

$$\begin{aligned}
|\psi\rangle|\xi\rangle &= \frac{1}{\sqrt{d}}\sum_{k,j=0}^{d-1} |\psi_k\rangle_{X_1}|\pi_j\rangle_{P_1}|\psi_k\rangle_{X_2}|\pi_j\rangle_{P_2}\cdots|\psi_k\rangle_{X_N}|\pi_j\rangle_{P_N}|\phi_j\rangle_{C_1C_2\cdots C_M} \\
&= \frac{1}{d^{(N+1)/2}}\sum_{m,n_1,n_2,\cdots,n_N}^{d-1} |\Phi_{m,n_1}\rangle|\Phi_{m,n_2}\rangle\cdots|\Phi_{m,n_N}\rangle \otimes \sum_{k}^{d-1} exp\Big[-i\frac{2\pi k}{d}(n_1+n_2+\cdots+n_N)\Big]\alpha_k|\phi_{k+m}\rangle
\end{aligned} \tag{265}$$

The following steps are involved in this protocol:

1. The senders performed a joint Bell-type measurement on particles X_j and P_j and get the outcomes, $|\Phi_{m,n_1}\rangle, |\Phi_{m,n_2}\rangle, \cdots, |\Phi_{m,n_1}\rangle$,
2. The outcomes were sent to the receivers by using classical communication,
3. Then, the receivers performe a local recovery unitary operator(LRUO) that satisfies $U_{m;n_1,n_2,\cdots,n_N}|\phi_{k+m}\rangle = exp\Big[i\frac{2\pi k}{d}(n_1+n_2+\cdots+n_N)\Big]|\phi_k\rangle$.

Several remarks are here: (i). In case that local operations are allowed, state $|\psi\rangle_X$ can be transformed locally to just one qudit, $\sum_{k=0}^{d-1}\alpha_k|\psi_k\rangle$. (ii). The M receivers are located in spatially separated places, otherwise if they are in the same port, local quantum operations can reversely change the qudit $\sum_{k=0}^{d-1}\alpha_k|\psi_k\rangle$ to a generalized GHZ like state shared by M parties. (iii). The scheme presented above combines the quantum information distribution and the teleportation together.

B. Symmetric $1 \to M$ telecloning

In this subsection, we study the $1 \to M$ generalized telecloning of qudit which is studied in (Murao *et al.*, 2000). In that scenario, the quantum information of d-level particle is transmitted optimally from one sender X to M receivers

$C_1, C_2, \cdots, C_M$. One "port" and $(M-1)$ ancillary particles were involved. The resource, including the port particle and $(2M-1)$ output states (M receivers and $(M-1)$ ancillas), is the maximally entangled state,

$$
\begin{aligned}
|\xi\rangle &= \frac{1}{\sqrt{d[M]}} \sum_{k=0}^{d[M]-1} |\xi_k^M\rangle_{PA} |\xi_k^M\rangle_C \\
&= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_P \otimes \Big(\frac{\sqrt{d}}{\sqrt{d[M]}} \sum_{k=0}^{d[M]-1} {}_P\langle j|\xi_k^M\rangle_{PA} |\xi_k^M\rangle_C \Big) \\
&= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_P \otimes |\phi_j\rangle, \qquad (266)
\end{aligned}
$$

where, $d[M] = C_{N+d-1}^N$, we denote the normalized symmetric state as, $|\xi_k^M\rangle = \frac{1}{\sqrt{\mathcal{N}(\xi_k^M)}} |\mathcal{P}(a_0, a_1, \cdots, a_{M-1})\rangle$, ($\mathcal{P}$ denotes the sum of all possible permutation of the elements $\{a_0, a_1, \cdots, a_{M-1}\}$ for $a_j \in \{0, 1, \cdots, d-1\}$ and $a_{j+1} > a_j$), $\{|\phi_j\rangle = \frac{\sqrt{d}}{\sqrt{d[M]}} \sum_{k=0}^{d[M]-1} {}_P\langle j|\xi_k^M\rangle_{PA} |\xi_k^M\rangle_C\}$ is a basis of the output state. The LRUO that satisfies $U_{mn}|\phi_{j+m}\rangle = e^{i\frac{2\pi nj}{d}}|\phi_j\rangle$ for the output state $\{|\phi_j\rangle\}$ is

$$
U_{mn} = \underbrace{U_{mn}^A \otimes \cdots \otimes U_{mn}^A}_{M-1} \otimes \underbrace{U_{mn}^C \otimes \cdots \otimes U_{mn}^c}_{M}, \qquad (267)
$$

where

$$
U_{mn}^A = \sum_{j=0}^{d-1} e^{-i\frac{2\pi jn}{d}} |j\rangle\langle j+m|, U_{mn}^C = \sum_{j=0}^{d-1} e^{i\frac{2\pi jn}{d}} |j\rangle\langle j+m| \qquad (268)
$$

The initial state $|\psi\rangle_X = \sum_{j=0}^{d-1} \alpha_j |j\rangle$ of the sender X is "encoded" to the separated output state $|\phi\rangle_X = \sum_{j=0}^{d-1} \alpha_j |\phi_j\rangle$ held by the (M-1) ancillas and M receivers.

$$
|\xi_k^M\rangle = \frac{1}{\sqrt{\mathcal{N}(\xi_k^M)}} |\mathcal{P}(a_0, a_1, \cdots, a_{M-1})\rangle = \frac{1}{\sqrt{\mathcal{N}(\xi_k^M)}} \sum_{a_j} \sqrt{\mathcal{N}(\xi_k'^{M-1})} |a_j\rangle |\xi_{k'}^{M-1}\rangle, \qquad (269)
$$

where $k' = f_M(a_0, \cdots, a_{j-1}, a_j, \cdots, a_{M-1})$. There is a relationship between index k and k': $k = g(a_j, k')$, then the total system takes the form,

$$
|\phi_j\rangle = \frac{\sqrt{d}}{\sqrt{d[M]}} \sum_{k'=0}^{d[M-1]-1} R_j^{k'} |\xi_{k'}^{M-1}\rangle_A \otimes |\xi_{g(j,k')}^M\rangle_C, \qquad (270)
$$

where we use the notation, $R_j^{k'} = \frac{\sqrt{\mathcal{N}(\xi_{k'}^{M-1})}}{\sqrt{\mathcal{N}(\xi_{g(j,k')}^M)}}$. By tracing out the ancillary states A, we obtain the output state of M qudits,

$$
\begin{aligned}
\rho_C =& tr_A(|\phi\rangle\langle\phi|) = \sum_{l=0}^{d[M-1]-1} {}_A\langle \xi_l^{M-1}|\phi\rangle\langle\phi|\xi_l^{M-1}\rangle_A \\
&= \frac{d}{d[M]} \sum_{j,j'=0}^{d-1} \sum_{k'=0}^{d[M-1]-1} \alpha_j \alpha_{j'}^* R_j^{k'} R_{j'}^{k'} |\xi_{g(j,k')}^M\rangle_C \langle \xi_{g(j,k')}^M| \\
&= \frac{d[1]}{d[M]} \Big(\sum_{k=0}^{d[M]-1} |\xi_k^M\rangle\langle\xi_k^M| \Big) \Big(|\psi\rangle\langle\psi| \otimes \mathbb{I}^{\otimes(M-1)} \Big) \Big(\sum_{k'=0}^{d[M]-1} |\xi_{k'}^M\rangle\langle\xi'^M_k| \Big) \\
&= \frac{d[1]}{d[M]} s_M(|\psi\rangle\langle\psi| \otimes \mathbb{I}^{\otimes(M-1)}) s_M = \hat{T}(|\psi\rangle\langle\psi|) \qquad (271)
\end{aligned}
$$

This reduced density matrix of the receivers is consistent with the density matrix for $1 \to M$ d-level optimal clones (Wang *et al.*, 2011b; Werner, 1998). Let us emphasize that the output of M qudits are consistent with optimal cloning, moreover, they are spatially separated in different places. The $1 \to M$ telecloning is also related with programming protocol which is studied in (Ishizaka and Hiroshima, 2008).

C. Economical phase-covariant telecloning

Quantum cloning machines have economic and non-economic cases. Similarly, we also have the economic telecloning (Wang and Yang, 2009a,b). We know that phase-covariant cloning has been studied in (Bruß *et al.*, 2000a; D'Ariano and Macchiavello, 2003; Fan *et al.*, 2003, 2001b). The $1 \to M$ optimal economical phase-covariant cloning for qubits was proposed in (Yu *et al.*, 2007), and the $1 \to 2$ economic map (non-optimal) for qudits also was studied (Durt *et al.*, 2005). For special value $M = kd + N$, the optimal $N \to M$ economical cloning for qudits has been introduced (Buscemi *et al.*, 2005). A protocol for the $1 \to M$ economical phase-covariant telecloning of qubits has been demonstrated in (Wang and Yang, 2009a), and the $1 \to 2$ economical phase cloning of qudits has been derived in (Wang and Yang, 2009b).

We next see the $1 \to M$ economical phase cloning of qubits, the input state is, $|\psi\rangle_X = \cos\frac{\theta}{2}|0\rangle_X + e^{i\phi}\sin\frac{\theta}{2}|1\rangle_X$:

$$\begin{cases} U|0\rangle_1|R_{2\cdots M}\rangle & = |\phi_0\rangle = |00\cdots 0\rangle_M \\ U|1\rangle_1|R_{2\cdots M}\rangle & = |\phi_1\rangle = \frac{1}{\sqrt{M}}\sum_{j=1}^{M}|0\cdots 1_j\cdots 0\rangle_M \end{cases}$$

We get the output state which is $|\psi\rangle_M^{out} = \cos\frac{\theta}{2}|\phi_0\rangle_X + e^{i\phi}\sin\frac{\theta}{2}|\phi_1\rangle_X$, and fidelity $F = {}_X\langle\psi|tr(|\psi\rangle_{out}\langle\psi|)|\psi\rangle_X = \frac{1}{M}\sin^4\frac{\theta}{2} + \cos^4\frac{\theta}{2} + \sin^2\frac{\theta}{2}\cos^2\frac{\theta}{2}\left(\frac{2}{\sqrt{M}} + \frac{M-1}{M}\right)$. Second, the telecloning scheme is that the sender X prepares the quantum information channel $|\xi\rangle_{PC} = \frac{1}{\sqrt{2}}\big(|0\rangle_P|\phi_0\rangle_C + |1\rangle_P|\phi_1\rangle_C\big)$. The total state can be expressed as

$$\begin{aligned} |\Psi\rangle_{XPC} = |\psi\rangle_X|\xi\rangle_{PC} = \frac{1}{2}\Big[& |\Phi^0\rangle_{XP}\otimes(\cos\frac{\theta}{2}|\phi_0\rangle + e^{i\phi}\sin\frac{\theta}{2}|\phi_1\rangle) + |\Phi^1\rangle_{XP}\otimes(\cos\frac{\theta}{2}|\phi_0\rangle - e^{i\phi}\sin\frac{\theta}{2}|\phi_1\rangle) \\ & + |\Phi^2\rangle_{XP}\otimes(e^{i\phi}\sin\frac{\theta}{2}|\phi_0\rangle + \cos\frac{\theta}{2}|\phi_1\rangle) + |\Phi^3\rangle_{XP}\otimes(e^{i\phi}\sin\frac{\theta}{2}|\phi_0\rangle - \cos\frac{\theta}{2}|\phi_1\rangle)\Big], \end{aligned} \tag{272}$$

where $\{|\Phi^0\rangle = |\Phi^+\rangle, |\Phi^1\rangle = |\Phi^-\rangle, |\Phi^2\rangle = |\Psi^+\rangle, |\Phi^3\rangle = |\Psi^-\rangle\}$ are the Bell basis. The next steps have been reviewed above in the generalized telecloning.

For the input state $|\psi\rangle_X = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} e^{i\theta_j}|j\rangle_X$, the $1 \to 2$ economical phase-covariant cloning machine was demonstrated in (Durt *et al.*, 2005). It takes the form,

$$\begin{cases} U|0\rangle_X|R\rangle = |\phi_0\rangle = |00\rangle \\ U|j\rangle_X|R\rangle = |\phi_j\rangle = \frac{1}{\sqrt{2}}(|j0\rangle + |0j\rangle), \quad (j \neq 0) \end{cases} \tag{273}$$

The fidelity is $F_{econ} = {}_X\langle\psi|tr(|\psi\rangle_{out}\langle\psi|)|\psi\rangle_X = \frac{1}{2d^2}[(d-1)^2 + (1+2\sqrt{2})(d-1) + 2]$. However, the optimal fidelity of $1 \to 2$ phase-covariant (with an ancilla) presented in (Fan *et al.*, 2003) is, $F_{opt} = \frac{1}{4d}(d + 2 + \sqrt{d^2 + 4d - 4})$. When $d = 2$, $F_{econ} = F_{opt}$ and otherwise $d > 2$, $F_{econ} < F_{opt}$. It is possible to achieve with optimal fidelity F_{opt} probabilistically (Wang and Yang, 2009b). In this scheme, the entangled state used is $|\xi\rangle_{PC} = \sum_{j=0}^{d-1} x_j|j\rangle_P|\phi_j\rangle_C$, where the coefficients x_j, that are assumed to be real numbers, satisfy the normalization condition $\sum_{j=0}^{d-1} x_j^2 = 1$. The quantum state of the whole system is,

$$|\Psi\rangle_{XPC} = |\psi\rangle_X \otimes |\xi\rangle_{PC} = \frac{1}{d}\sum_{m,n=0}^{d-1}|\Phi_{mn}\rangle_{XP}\sum_{j=0}^{d-1}\exp\big(i\frac{2\pi nj}{d}\big)x_{j+m}e^{i\theta_j}|\phi_{j+m}\rangle_C \tag{274}$$

Only when the outcome of the Bell-type joint measurement is $\{m = 0, n\}$(with probability $1/d$), the receivers can obtain the clones $|\psi\rangle_{out} = \sum_{j=0}^{d-1} x_j e^{i\theta_j}|\phi_j\rangle$ by using the LRUO $U = U_{0n}\otimes\mathbb{I}$. The fidelity of this clones is $F^t_{econ} = \frac{1}{d}\Big(1 + \sqrt{2}x_0\sum_{j=0}^{d-1}x_j + \sum_{i=1}^{d-2}\sum_{j=i+1}^{d-1}x_i x_j\Big)$. We set $\{x_j\}$ as

$$\begin{aligned} x_0 &= X(d) = \sqrt{\frac{4(d-1)}{D(D+d-2)}}, \\ x_j &= Y(d) = \sqrt{\frac{d^2 + (d-2)D}{D(D+d-2)(d-1)}}, \quad (j \neq 0), \end{aligned} \tag{275}$$

where $D = \sqrt{d^2 + 4d - 4}$. It's not difficult to verify that $F^t_{econ} = F_{opt}$ for any d. Actually, the output state of this telecloning scheme is equivalent to the ρ^C_{opt} of the optimal phase-covariant cloning after tracing out of the ancilla

(Fan *et al.*, 2003). For $d>2$, the von Neumann entropy $S(|\xi\rangle\langle\xi|) = -X^2(d)\log_2 X^2(d) - (d-1)Y^2(d)\log_2 Y^2(d) < \log_2 d$, which implies $|\xi\rangle$ is only partially entangled. Thus, we can conclude that the suitable quantum entanglement in realizing the optimal $1\to 2$ cloning of qudits with a certain probability $1/d$ are special configurations of nonmaximally entangled states rather than the maximally entangled states.

D. Asymmetric telecloning

Quantum telecloning described in the previous section evenly distributes information of the unknown input state to the distant receivers. However, it may be desirable to transmit information to several different receivers with different fidelities. For example, the sender Alice trusts Bob more than Claire hope Bob's fidelity is larger. These schemes are asymmetric telecloning. The 1 to 2 optimal asymmetric quantum cloning of qubits was introduced in (Bužek *et al.*, 1998; Cerf, 1998, 2000b; Niu and Griffiths, 1998). The 1 to 2 asymmetric cloning machine was generalized to d-dimension case in (Braunstein *et al.*, 2001b; Cerf, 2000a), and recently in (Wang *et al.*, 2011b).

Here, we briefly review $1\to 2$ asymmetric telecloning for qubits (Murao *et al.*, 2000) as an example. The entanglement state resource is, $|\xi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_P|\phi_0\rangle + |1\rangle_P|\phi_1\rangle$, where

$$\begin{cases} |\phi_0\rangle &= \frac{1}{\sqrt{1+p^2+q^2}}(|0\rangle|0\rangle_B|0\rangle_C + p|1\rangle|0\rangle_B 1\rangle_C + q|1\rangle|1\rangle_B|0\rangle_C) \\ |\phi_1\rangle &= \frac{1}{\sqrt{1+p^2+q^2}}(|1\rangle|1\rangle_B|1\rangle_C + p|0\rangle|1\rangle_B 0\rangle_C + q|0\rangle|0\rangle_B|1\rangle_C) \quad (p+q=1) \end{cases} \tag{276}$$

The LRUOs satisfy the conditions, $\sigma_z\otimes\sigma_z\otimes\sigma_z|\phi_{0(1)}\rangle = (-)|\phi_{0(1)}\rangle, \sigma_x\otimes\sigma_x\otimes\sigma_x|\phi_{0(1)}\rangle = |\phi_{1(0)}\rangle$. And the final output state is $|\psi\rangle_{out} = \alpha_0|\phi_0\rangle + \alpha_1|\phi_1\rangle$ while the input state being $|\psi\rangle_X = \alpha_0|0\rangle + \alpha_1|1\rangle$. The fidelities of Bob and Claire, which satisfy the trade-off relation, $\sqrt{(1-F_B)(1-F_C)} = F_B + F_C - \frac{3}{2}$, respectively are

$$F_B = \frac{1+p^2}{1+p^2+q^2} \quad F_C = \frac{1+q^2}{1+p^2+q^2}. \tag{277}$$

Next, we show the results of 1 to 2 asymmetric telecloning of qudits. The asymmetric cloning machine is

$$U|j\rangle_{C_1}|00\rangle_{C_2A} = |\phi_j\rangle = \sum_{m,n=0}^{d-1}\beta_{m,n}(V_{m,n}|j\rangle_{C_1})\otimes|\Phi_{m,-n}\rangle_{C_2A} \tag{278}$$

$$= \sum_{m,r=0}^{d-1} b_{m,r}|j+m\rangle_{C_1}|j+r\rangle_{C_2}|j+m+r\rangle_A, \tag{279}$$

where $V_{m,n} = \sum_{j=0}^{d-1} e^{2\pi jn/d}|j+m\rangle\langle j|$ are generalized Pauli matrices and $b_{m,r} = \frac{1}{\sqrt{d}}\sum_{n=0}^{d-1} e^{-i2\pi nr/d}\beta_{m,n}$. We have a mathematical equation,

$$\sum_{m,n=0}^{d-1}\beta_{m,n}|\Phi_{m,n}\rangle_{RC_1}|\Phi_{m,-n}\rangle_{C_2A} = \sum_{m,n=0}^{d-1}\gamma_{m,n}|\Phi_{m,n}\rangle_{RC_2}|\Phi_{m,-n}\rangle_{C_1A} \tag{280}$$

where $\sum_{m,n=0}^{d-1}|\beta_{m,n}|^2 = 1$, $\gamma_{m,n} = \frac{1}{d}\sum_{x,y=0}^{d-1} e^{i2\pi(nx-my)/d}\beta_{x,y}$. Then we project this equation on $|j\rangle_R$ and get $|\phi_j\rangle = \sum_{m,n=0}^{d-1}\gamma_{m,n}(V_{m,n}|j\rangle_{C_2})\otimes|\Phi_{m,-n}\rangle_{C_1A}$. The input state $|\psi\rangle_X = \sum_{j=0}^{d-1}\alpha_j|j\rangle$ is copied into the output states $|\psi\rangle_{out} = \sum_{j=0}^{d-1}\alpha_j|\phi_j\rangle_{C_1C_2A}$. This output states are described by the reduced density matrices, respectively,

$$\rho_{C_1} = tr_{C_2A}(|\psi\rangle_{out}\langle\psi|) = \sum_{m,n=0}^{d-1}|\beta_{m,n}|^2 V_{m,n}|\psi\rangle_X\langle\psi|V_{m,n}^\dagger, \tag{281}$$

$$\rho_{C_2} = tr_{C_1A}(|\psi\rangle_{out}\langle\psi|) = \sum_{m,n=0}^{d-1}|\gamma_{m,n}|^2 V_{m,n}|\psi\rangle_X\langle\psi|V_{m,n}^\dagger. \tag{282}$$

In order to generate the clones that are characterized by the optimal fidelities which are independent of the input state, the following condition should be satisfied (Cerf, 2000a; Cerf *et al.*, 2002b),

$$\begin{aligned} b_{0,0} &= \frac{1}{\sqrt{d}}[\nu + (d-1)\mu], \quad b_{m,0} = \sqrt{d}\mu, \\ b_{0,r} &= \frac{1}{\sqrt{d}}(\nu-\mu), \quad b_{m,r} = 0, \quad (m\neq 0, r\neq 0) \end{aligned} \tag{283}$$

And we get the fidelities of two clones

$$F_{C_1} = \frac{1+(d-1)p^2}{1+(d-1)(p^2+q^2)}, \quad F_{C_2} = \frac{1+(d-1)q^2}{1+(d-1)(p^2+q^2)}, \tag{284}$$

where $p = \frac{\nu-\mu}{\nu+(d-1)\mu}, q = 1-p$. When $p = q = 1/2$, the fidelities are in agreement with $F = \frac{N(d-1+M)+M}{M(d+N)}(N = 1, M = 2)$ obtained by Werner (Werner, 1998). The telecloning scheme requires the quantum entanglement, shared by the port, ancilla, and the receivers C_1, C_2, is given as $|\xi\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle_P|\phi_j\rangle_{C_1C_2A}$. After the sender performs a Bell-type joint measurement on the input and port particles, and gets the result m, n, the ancilla and the receivers C_1, C_2 perform the LRUO $U_{m,n}^{local} = \sum_{j_1,j_2,j_3} e^{i2\pi n(j_1+j_2-j_3)/d}|j_1\rangle\langle j_1+m|_{C_1}\otimes|j_2\rangle\langle j_2+m|_{C_2}\otimes|j_3\rangle\langle j_3+m|_A$ and gets the output state $|\psi\rangle_{out} = \sum_{j=0}^{d-1}\alpha_j|\phi_j\rangle_{C_1C_2A}$.

E. General telecloning

In the general case (Zhang *et al.*, 2013), the sender hold the N identical input states at the same location as $|\psi\rangle_X = \sum_{\vec{n}}^{N}(\sqrt{N!}\prod_j \frac{\alpha_j^{n_j}}{\sqrt{n_j!}})|\vec{n}\rangle = \sum_{\vec{n}}^{N} y_{\vec{n}}|\vec{n}\rangle$. The sender would like to distribute these states to spatially separated M receivers, $M \geq N$. Following the teleportation procedure, the sender performs a joint measurement on input particles $X_1, X_2, \cdots, X_N$ and port particles $P_1, P_2, \cdots, P_N$ which are acting as ancillary states, then announce the outcome to the $M-N$ ancillas and M receivers via classical communication. Next, the ancillas and receivers get the optimal clones after applying the specific Local Recovery Unitary Operator (LRUO). In order to achieve this aim, instead of using joint Bell-type measurement, the sender performs a more general positive operator-valued measure (POVM) on the system,

$$|\chi(\vec{x})\rangle = [\mathbb{I}_X^{\otimes N}\otimes U(\vec{x})_P^{\otimes N}]\frac{1}{\sqrt{d[N]}}\sum_{\vec{n}}^{N}|\vec{n}\rangle_X|\vec{n}\rangle_P, \tag{285}$$

$$\int d\vec{x}F_{\vec{x}} = \int d\vec{x}\lambda(\vec{x})|\chi(\vec{x})\rangle\langle\chi(\vec{x})| = S_X^N\otimes S_P^N \tag{286}$$

where $S^N\otimes S^N$ is the identity in the space $\mathcal{H}_+^{\otimes N}\otimes\mathcal{H}_+^{\otimes N}$, $U(\vec{x})$ is an element of Lie group $SU(d)$, and the vector $\vec{x}$ consisting (d^2-1) parameters which can determine the unitary operator. Next we show that the latter equation can be satisfied. According to the theorem of Weyl Reciprocity (Ma, 2007), the unitary transformation $U^{\otimes N}$ and permutation permutation P_α can be exchanged. If $\mathcal{Y}_\mu^{[\lambda]}$ is a standard Young operator corresponding to the standard Young tableau with N boxes, the subspace $\mathcal{Y}_\mu^{[\lambda]}\mathcal{H}^{\otimes N}$ will be invariant under transformation $U^{\otimes N}$. Considering that the symmetric projection S^N is equal to the standard Young operator $\frac{1}{N!}\mathcal{Y}^{[N]}$, we have

$$U(\vec{x})^{\otimes N}S^N = S^N U(\vec{x})^{\otimes N}, \tag{287}$$

$$U(\vec{x})^{\otimes N}|\vec{n_1}\rangle = \sum_{\vec{n_2}} D_{\vec{n_2},\vec{n_1}}(\vec{x})|\vec{n_2}\rangle, \tag{288}$$

where $D(\vec{x})$ is a representation of Lie group $SU(d)$. A group theorem states that an irreducible representation of group $SU(d)$ will be induced when $U(\vec{x})^{\otimes N}$ operates on invariant subspace $\mathcal{Y}_\mu^{[\lambda]}\mathcal{H}^{\otimes N}$ when $\mathcal{Y}_\mu^{[\lambda]}$ is a standard Young operator, see (Ma, 2007). Thus $D(\vec{x})$ is an irreducible representation of group $SU(d)$. Then according to Schur's lemmas and the orthogonality relations (Ma, 2007), we obtain,

$$\frac{1}{d[N]}\int d\vec{x}\lambda(\vec{x})D_{\vec{n_1},\vec{n_2}}(\vec{x})D^*_{\vec{n_3},\vec{n_4}}(\vec{x}) = \delta_{\vec{n_1},\vec{n_3}}\delta_{\vec{n_2},\vec{n_4}} \tag{289}$$

This formula ensures that the integral of the projectors $F_{\vec{x}}$ is equal to the identity operator in the space $\mathcal{H}_+^{\otimes N}\otimes\mathcal{H}_+^{\otimes N}$ which should be satisfied for a POVM. In special case $d = 2$, because we know the analytical expression of the unitary matrix $U(\vec{x})$ and its irreducible representation $D(\vec{x})$, an appropriate finite POVM can be constructed, then the integral reduces to summation. The importance to construct finite POVM is that its explicit form is necessary for experimental implementation.

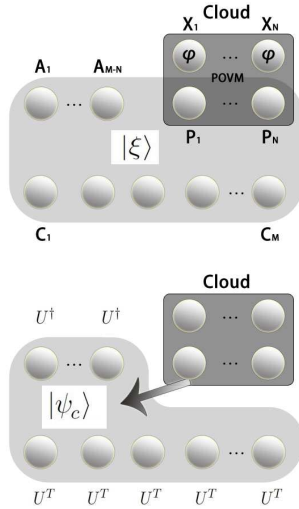


FIG. 6 Scheme of telecloning. The sender who may possess several ports share a maximally entangled state with several receivers who are spatially separated, and possibly assisted with ancillary states. The sender (Cloud) performs a POVM and announces the measurement result, the receiver can recover their states locally, see (Zhang *et al.*, 2013)

The total system can be expressed as

$$\begin{aligned} |\psi\rangle_X|\xi\rangle_{PAC} &= \frac{1}{d[N]}\sum_{\vec{x}}\lambda(\vec{x})|\chi(\vec{x})\rangle_{XP}[U^\dagger(\vec{x})_A^{\otimes(M-N)}\otimes U^T(\vec{x})_C^{\otimes M}]^\dagger\sqrt{\frac{d[N]}{d[M]}}\Big(\sum_{\vec{n}}^{N} y_{\vec{n}}\ {}_P\langle\vec{n}|\Big)\Big(\sum_{\vec{m}}^{M}|\vec{m}\rangle_{PA}|\vec{m}\rangle_C\Big) \\ &= \frac{1}{d[N]}\sum_{\vec{x}}\lambda(\vec{x})|\chi(\vec{x})\rangle_{XP}[U^{local}(\vec{x})]^\dagger|\psi_c\rangle_{AC} \end{aligned} \tag{290}$$

The LRUO is $U^{local}(\vec{x}) = U^\dagger(\vec{x})_A^{\otimes(M-N)}\otimes U^T(\vec{x})_C^{\otimes M}$. As we expect, the sender distributes the universal cloning state $|\psi_c\rangle_{AC}$ to spatially separated M receivers assisted by $(M-N)$ ancillas. The scheme of the telecloning can be represented in FIG.6.

The asymmetric quantum telecloning for multiqubit states with various figures of merit are investigated by Chen and Chen (Chen and Chen, 2007a). The reverse processing of telecloning is the remote state concentration. Roughly speaking, The final state of the information concentration is the initial state of the telecloning. It is shown that in the concentration processing, the bound entangled state can be used as a resource (Murao and Vedral, 2001). On the other hand, the standard entangled state can also be used with similar capability in the quantum information concentration (Zhang *et al.*, 2013). This remote quantum information concentration is also studied in (Wang *et al.*, 2011a). The experimental realization of telecloning is performed by partial teleportation scheme (Zhao *et al.*, 2005). A proposal of distance cloning is in (Filip, 2004b). The entanglement resource of up to six qubits of Dicke states is created experimentally (Prevedel *et al.*, 2009). The experimental implementation of telecloning of optical coherent states is demonstrated in (Koike *et al.*, 2006). The experimental telecloning of phase-conjugate inputs is presented in (Zhang *et al.*, 2008). Telecloning of entanglement is presented in (Ghiu and Karlsson, 2005), the telecloning of W state is studied in (Yan *et al.*, 2009). A scheme to implement an economical phase-covariant quantum telecloning is separate cavities is proposed in (Fang *et al.*, 2012b). Implementation of telecloning of economic phase-covariant about bipartite entangled state is studied in (Meng and Zhu, 2009). The continuous variable telecloning with bright entangled beams is studied in (Olivares and Paris, 2008). The controlled telecloning and teleflipping for one pure qubit is studied in (Zhan *et al.*, 2009).

VIII. QUANTUM CLONING FOR CONTINUOUS VARIABLE SYSTEMS

This section is devoted to the issue of quantum cloning machine (QCM) for continuous variable systems. The available reviews are (Scarani *et al.*, 2005) and (Cerf and Grangier, 2007). An example of continuous systems is simply to consider the position and momentum of a particle, or the two quadratures of a quantized electromagnetic field. Instead of universal cloning, we only study the case of $N \to M$ Gaussian cloning for coherent states, whose precise definition will be given in the context later. We shall first get the fidelity bound for $N \to M$ Gaussian cloning(Cerf and Iblisdir, 2000), and then give an explicit implementation using a linear amplifier and beam splitters(Braunstein *et al.*, 2001a). Note that the same procedure is also suitable if the input states are squeezed states, provided little change of parameters of the devices is made(Braunstein *et al.*, 2001a; Cerf and Iblisdir, 2000).

A. Optimal bounds for Gaussian cloners of coherent states

We deal with a quantum system described in terms of two canonically conjugated operators $\hat{x}$ and $\hat{p}$, which respectively has a continuous spectra. Since $\hat{x}$ and $\hat{p}$ are conjugated, they cannot both be copied perfectly, so we hope to find a cloning machine which makes an approximately cloning and get an "optimal" result. Corresponding to universal cloning, we here focus on cloning transformations which take only coherent states as input, that is, the input states of the cloning machine form a set $\mathcal{S}$, which can be parametrized as,

$$\mathcal{S} = \left\{ |\alpha\rangle : \alpha = \frac{1}{\sqrt{2}}(x+ip), x, p \in \boldsymbol{R} \right\}, \tag{291}$$

where $\langle\alpha|\hat{x}|\alpha\rangle = x$ and $\langle\alpha|\hat{p}|\alpha\rangle = p$. Moreover we shall only consider $N \to M$ symmetric Gaussian cloners(SGCs) which can be defined as a linear completely positive map:$C_{N,M} : \mathcal{H}^{\otimes N} \to \mathcal{H}^{\otimes M}$, where $\mathcal{H}$ stands for an infinite-dimensional Hilbert space. So after the transformation we shall get $\rho_M = C_{N,M}(|\alpha\rangle\langle\alpha|^{\otimes N})$. To mean Gaussian, the reduced state of a single clone needs to satisfy:

$$\begin{aligned} \rho_1 &= Tr_{M-1}(\rho_M) \\ &= \frac{1}{\pi\sigma_{N,M}^2} \int d^2\beta e^{-|\beta|^2/\sigma_{N,M}^2} D(\beta)|\Psi\rangle\langle\Psi|D^\dagger(\beta), \end{aligned} \tag{292}$$

where the integral is performed over all values of $\beta = (x+ip)/\sqrt{2}$ in the complex plane, note that we have set $\hbar = 1$, and $D(\beta) = exp(\beta\hat{a}^\dagger - \beta^*\hat{a})$ is a displacement operator which shifts a state of x in position and p in momentum, $\hat{a}$ and $\hat{a}^\dagger$ denote annihilation and creation operators respectively. As a result, after cloning for each copy an extra noise $\sigma_x^2 = \sigma_p^2 = \sigma_{N,M}^2$on the conjugate variables x and p are added. It is readily checked that the cloning fidelity $f_{N,M} = \langle\alpha|\rho_1|\alpha\rangle$ is the same for any coherent input state $|\alpha\rangle$, provided $\sigma_{N,M}$ remains invariant, which means, our cloner is symmetric. Through simple computation one finds,

$$f_{N,M} = \langle\alpha|\rho_1|\alpha\rangle = \frac{1}{1+\sigma_{N,M}^2}. \tag{293}$$

Now we shall make the proposition that the lower bound of $\sigma_{N,M}$ is

$$\bar{\sigma}_{N,M}^2 = \frac{M-N}{MN}, \tag{294}$$

which implies the optimal fidelity for $N \to M$ cloning machine is

$$f_{N,M} = \frac{1}{1+\bar{\sigma}_{N,M}^2} = \frac{MN}{MN+M-N}. \tag{295}$$

Next we will prove (294). As first step we shall come up with a lemma.

Lemma 1. Cascading a $N \to M$ cloner with an $M \to L$ cloner cannot be better than the optimal $N \to L$ cloner. In our case, two cascading $N \to M$ and $M \to L$ SGCs result in a single $N \to L$ SGC whose variance is simply the sum of variances of the two cascading SGCs. Hence we have

$$\bar{\sigma}_{N,L}^2 \le \sigma_{N,M}^2 + \sigma_{M,L}^2, \tag{296}$$

where $\bar{\sigma}_{N,M}^2$ stands for the low variance bound of $N \to L$ cloner.

The proof for Lemma 1 can be found in (Cerf and Iblisdir, 2000). We will use lemma 1 to reach (294). From (296), setting $L \to \infty$ we get

$$\bar{\sigma}^2_{N,\infty} \leq \sigma^2_{N,M} + \bar{\sigma}^2_{M,\infty}. \tag{297}$$

Then we can use quantum estimation theory to analyze $\bar{\sigma}^2_{N,\infty}$, which is the variance of an optimal joint measurement of $\hat{x}$ and $\hat{p}$ on N replicas of a system. We have (Holevo, 1982),

$$g_x \sigma_x^2(1) + g_p \sigma_p^2(1) \geq g_x \Delta \hat{x}^2 + g_p \Delta \hat{p}^2 + \sqrt{g_x g_p}, \tag{298}$$

for all values of the constants $g_x, g_p > 0$, where $\sigma_x^2(1)$ and $\sigma_p^2(1)$ denote the variance of the measured values of $\hat{x}$ and $\hat{p}$, while $\Delta\hat{x}^2$ and $\Delta\hat{p}^2$ denote the intrinsic variance of observables $\hat{x}$ and $\hat{p}$, respectively. For each value of g_x and g_p, we have a specific positive-operator-valued measure(POVM) which achieves the bound. Also, as in classical statistics, we have (Holevo, 1982),

$$\sigma_x^2(N) = \frac{\sigma_x^2(1)}{N}, \sigma_p^2(N) = \frac{\sigma_p^2(1)}{N}, \tag{299}$$

where $\sigma_x^2 N$ or $\sigma_p^2 N$ is the measured variance of $\hat{x}$ or $\hat{p}$ if we perform the measurement on N independent and identical systems. In the context of coherent states, $\Delta\hat{x}^2 = \Delta\hat{p}^2 = 1/2$, if we further require $\sigma_x^2(N) = \sigma_p^2(N)$, the tight bound of (298) is reached for $g_x = g_p$. Then it yields from (298)

$$\bar{\sigma}^2_{N,\infty} = 1/N. \tag{300}$$

Combine (300) and (296), we have completed our proof.

B. Implementation of optimal Gaussian QCM with a linear amplifier and beam splitters

In this section, we shall give the explicit transformation for the optimal Gaussian $N \to M$ cloning of coherent states, and show that the transformation can be implemented through the common devices used in quantum optics experiments: a phase-insensitive linear amplifier and a network of beam splitters(Braunstein *et al.*, 2001a). Thus we can prove that the optimal bounds of fidelity derived in the previous section can actually be achieved. Note also other implementations may be possible as well, for example, a scheme using a circuit of CNOT gates is proposed to be an implementation for the $1 \to 2$ Gaussian cloning(Cerf *et al.*, 2000).

Assume the state to be cloned is $|\alpha\rangle$, we denote the initial input state of the cloning machine as $|\Psi\rangle = |\alpha\rangle^{\otimes N} \otimes |0\rangle^{\otimes M-N} \otimes |0\rangle_z$, where except the N input modes to be cloned, we have $M-N$ blank modes and an ancillary mode z. The blank modes and the ancilla are prepared initially in the vacuum state $|0\rangle$. Let $\{x_k, p_k\}$ denote the pair of quadrature operators associated with each mode k involved in the cloning transformation, where $k = 0, ..., M-1$(for simplicity, we sometimes omit the hats for operators when the context is unambiguous). As usual, for cloning we mean a quantum operation $U : \mathcal{H}^{\otimes M-1} \to \mathcal{H}^{\otimes M-1}$ performed on the initial state $|\Psi\rangle$, and the output state becomes $|\Psi''\rangle = U|\Psi\rangle$.

For simplicity of analysis and calculation which shall be shown below, we work in the Heisenberg picture, then U can be described by a canonical transformation acting on the operators $\{x_k, p_k\}$:

$$x_k'' = U^\dagger x_k U, \quad p_k'' = U^\dagger p_k U, \tag{301}$$

while the state $|\Psi\rangle$ is left invariant. We will now impose several requirements for the transformation U which establish some expected properties of the state after cloning:

1. The expected values of x and k for the M output modes be:

$$\langle x_k'' \rangle = \langle \alpha | x_0 | \alpha \rangle, \quad \langle p_k'' \rangle = \langle \alpha | p_0 | \alpha \rangle, \tag{302}$$

   which means the state of the clones is centered on the original coherent state.

2. Note that for a coherent state, we have $\sigma_x^2 = \sigma_p^2 = \Delta x_{vac}^2 = \frac{1}{2}$, and also by a rotation in the phase space, we get the operator $v = cx + dp$, (where c and d are complex numbers satisfying $|c|^2 + |d|^2 = 1$), the error variance of which is the same:

$$\sigma_v^2 = \sigma_x^2 = \sigma_p^2 = \Delta x_{vac}^2 = \frac{1}{2}. \tag{303}$$

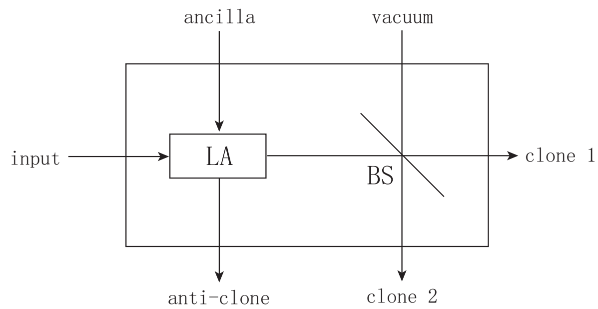


FIG. 7 Implementation of the optimal Gaussian $1 \rightarrow 2$ QCM for light modes. LA stands for linear amplifier and BS represents a balanced beam splitter, see (Braunstein *et al.*, 2001a).

We then require that the invariance property under rotation is preserved by the transformation U, which yields

$$\sigma^2_{v_k^{''}} = \sigma^2_{x_k^{''}} = \sigma^2_{p_k^{''}} = (1 + \frac{2}{N} - \frac{2}{M})\Delta x^2_{vac}, \tag{304}$$

where $v_k^{''} = cx_k^{''} + dp_k^{''}$.

3. U is unitary, which in the Heisenberg picture is equivalent to demand that the commutation relations are preserved through the transformation:

$$[x_j^{''}, x_k^{''}] = [p_j^{''}, p_k^{''}] = 0, \quad [x_j^{''}, p_k^{''}] = i\delta_{jk}, \tag{305}$$

for $j, k = 0, ..., M - 1$ and for the ancilla.

Based on the above requirements we shall then give the explicit implementation of the cloning machine.

C. Optimal $1 \rightarrow 2$ Gaussian QCM

We first consider the simple case of duplication ($N = 1, M = 2$). An explicit transformation can be found:

$$\begin{aligned} x_0^{''} &= x_0 + \frac{x_1}{\sqrt{2}} + \frac{x_z}{\sqrt{2}}, \quad p_0^{''} = p_0 + \frac{p_1}{\sqrt{2}} - \frac{p_z}{\sqrt{2}}, \\ x_1^{''} &= x_0 - \frac{x_1}{\sqrt{2}} + \frac{x_z}{\sqrt{2}}, \quad p_1^{''} = p_0 - \frac{p_1}{\sqrt{2}} - \frac{p_z}{\sqrt{2}}, \\ x_z^{'} &= x_0 + \sqrt{2}x_z, \quad p_z^{'} = -p_0 + \sqrt{2}p_z, \end{aligned} \tag{306}$$

for which one can check that all the three requirements are satisfied.

Next we proceed to see how to implement the above duplicator in practice. First interpret (306) as a sequence of two canonical transformations:

$$\begin{aligned} a_0^{'} &= \sqrt{2}a_0 + a_z^{\dagger}, \quad a_z^{'} = a_0^{\dagger} + \sqrt{2}a_z \\ a_0^{''} &= \frac{1}{\sqrt{2}}(a_0^{'} + a_1), \quad a_1^{''} = \frac{1}{\sqrt{2}}(a_0^{'} - a_1), \end{aligned} \tag{307}$$

where $a_k = (x_k + ip_k)/\sqrt{2}$ and $a_k^{\dagger} = (x_k - ip_k)/\sqrt{2}$ denote the annihilation and creation operators for mode k. We then can immediately come up with a practical scheme which has two steps to have the desired transformation realized. Step 1 is a phase-insensitive amplifier whose gain G is equal to 2, while step 2 is a phase-free 50:50 beam splitter(see Fig. 7). To see the cloner is optimal, we note from (Caves, 1982), for an amplifier of gain G, each quadrature's excess noise variance is bounded by

$$\sigma^2_{LA} \geq (G - 1)/2. \tag{308}$$

Since we have chosen G to be 2, it yields $\sigma^2_{LA} = 1/2$, which proves the optimality of the cloning transformation.

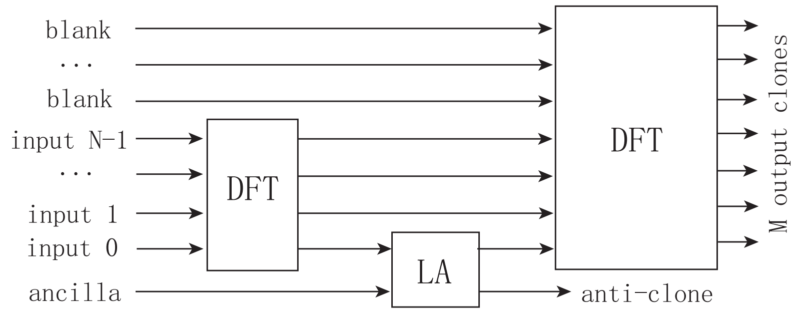


FIG. 8 Implementation of the optimal Gaussian $N \to M$ QCM for light modes. LA represents linear amplifier, DFT stands for discrete Fourier transform, see (Braunstein *et al.*, 2001a).

D. Optimal Gaussian $N \to M$ QCM

Now we continue to study the case of $N \to M$ Gaussian cloning, this time we shall again use linear amplifier to achieve the transformation. Due to the relation of extra variance and gain from (308), we need to make G as low as possible in order to reach the optimal limit of $\sigma^2_{N,M}$. The cloning procedure is as follows: (i)concentrate the N input modes to one single mode, which is then amplified. (ii) distribute the concentrated mode symmetrically among the M output modes. Obviously an easy method to realize the processes is through discrete Fourier transform (DFT), with which we can write out the detailed steps of the cloning procedure. Step 1: concentration of the N input modes by a DFT:

$$a_k^{'} = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} exp(ikl2\pi/N)a_l, \tag{309}$$

where $k = 0, ..., N-1$. After the concentration, the energy of the N input modes is put together on one single mode, which we shall rename as a_0, while every other mode become a vacuum state. Step 2: take the mode a_0 together with the ancilla as the input of a linear amplifier of gain $G = M/N$, which results,

$$\begin{aligned} a_0^{'} &= \sqrt{\frac{M}{N}} a_0 + \sqrt{\frac{M}{N} - 1} a_z^{\dagger}, \\ a_z^{'} &= \sqrt{\frac{M}{N} - 1} a_0^{\dagger} + \sqrt{\frac{M}{N}} a_z. \end{aligned} \tag{310}$$

Step 3: distribute energy symmetrically onto the M outputs by performing a DFT on $a_0^{'}$ and the $M-1$ vaccum modes produced in step 1:

$$a_k^{''} = \frac{1}{\sqrt{M}} \sum_{l=0}^{M-1} exp(ikl2\pi/M)a_l^{'}, \tag{311}$$

It's readily checked that the procedure can meet our three requirements. Moreover if we choose $\sigma^2_{LA} = [M/N - 1]/2$, the optimality is then confirmed.

Like the case of $1 \to 2$ cloning, we shall also use a network of beam splitters to construct the required DFT. It is shown that any discrete unitary operator can be experimentally realized by a sequence of beam splitters and phase shifters(Reck *et al.*, 1994). An explicit construction is given in (Braunstein *et al.*, 2001a).

E. Other developments and related topics

Experimental implementation of Gaussian cloning of coherent states with fidelity of about 65% by only linear optics is shown in (Andersen *et al.*, 2005), the results are further analyzed in (Olivares *et al.*, 2006). Similar as in discrete space case, if we know partial information of the input state in CV system, the fidelity can also be improved (Alexanian, 2006). Without analog in discrete case, the quantum cloning with phase-conjugate input modes is studied in (Cerf and Iblisdir, 2001b). By some figure of merit, the optimal cloning of coherent states with non-Gaussian setting may be better than a Gaussian setting (Cerf *et al.*, 2005). However, CV cryptography

(Grosshans and Grangier, 2002) is still secure under non-Gaussian attack (Grosshans and Cerf, 2004). The asymmetry CV cloning used for security analysis of cryptography is also discussed in (Cerf *et al.*, 2002c). The CV universal NOT gate is studied in (Cerf and Iblisdir, 2001a). The application of CV cloning machine in key distribution is studied in (Cerf *et al.*, 2001). The quantum cloning limits for finite distributions of coherent states are studied in (Cochrane *et al.*, 2004), and also in (Demkowicz-Dobrzanski *et al.*, 2004). The CV quantum cloning via various schemes are proposed in (Braunstein *et al.*, 2001a; D'Ariano *et al.*, 2001; Fiurášek, 2001b). The multicopy Gaussian states is in (Fiurasek and Cerf, 2007). The Gaussian cloning of coherent light states into an atomic quantum memory is presented in (Fiurášek *et al.*, 2004). The optimal cloning of mixed Gaussian states is studied in (Guta and Matsumoto, 2006). The superbroadcasting of CV mixed states is studied in (D'Ariano *et al.*, 2006). A proposal to test quantum limits of a Gaussian-distributed set of coherent state related with cloning is presented in (Namiki, 2011). The cloning of CV entangled state is studied in (Weedbrook *et al.*, 2008). Experimental realization of CV cloning with phase-conjugate inputs is shown in (Sabuncu *et al.*, 2007) and also in (Chen and Zhang, 2007). The CV teleportation is studied in (Braunstein *et al.*, 2000). The experimental realization of both CV teleportation and cloning is reported in (Zhang *et al.*, 2005). The criteria of CV cloning and teleportation are studied in (Grosshans and Grangier, 2001). The reviews of CV quantum information can be found in (Braunstein and van Loock, 2005; Wang *et al.*, 2007; Weedbrook *et al.*, 2012), the review of CV cloning and QKD can be found in (Cerf and Grangier, 2007).

IX. MEAN KING PROBLEM AS A QUANTUM KEY DISTRIBUTION PROTOCOL

In this section, we will study a quantum retrodiction scheme used for quantum key distribution. The results presented in this section are new.

A. Introduction of mean king problem

Quantum key distribution (QKD) protocols allow two parties, called Alice (the sender) and Bob (the receiver) conventionally, to generate shared secret keys for them to communicate securely. In BB84 protocol(Bennett and Brassard, 1984), we send states by exploiting two mutually unbiased bases of qubit. Ekert proposed a QKD protocol based on Bell theorem by using the entangled pairs in 1991 (E91) (Ekert, 1991). As we already know that the BB84 protocol can also be generalized by using a six-state protocol (Bruß, 1998).

In this Section, we will study a QKD protocol which is essentially a combination of BB84 protocol and E91 protocol, and it is based on the so-called mean king problem (Vaidman *et al.*, 1987) since its description is usually like a tale (Englert and Aharonov, 2001).

The protocol of mean king problem, which will be presented later in detail, can be considered as two steps: The first step is the same as E91 protocol except without classical announcement of measurement bases and the second step is like BB84 protocol. In this protocol, Bob needs to retrodict the outcome of a projective measurement by Alice without knowing the bases she used. For qubit first (Vaidman *et al.*, 1987) and higher dimension latter (Hayashi *et al.*, 2005; Kimura *et al.*, 2006), it is shown that Bob has a 100% winning strategy. So it is realized that this quantum retrodiction protocol might be applied as a QKD in quantum cryptography (Bub, 2001; Werner *et al.*, 2009; Yoshida *et al.*, 2010). However, one problem is that this QKD is shown to be secure only in transmission-error free scenario, it is not clear in other situations. As is well-known, the error caused by decoherence is inevitable in real physical system, in particular for entangled states which are necessary in this protocol. Another problem is that, compared with existing QKD protocols, it is not clear whether this quantum retrodiction protocol is more secure or not, or in general what is the advantage of it.

In this section, we study the QKD based on the retrodiction protocol by considering the attacks on both steps of the entangled pair preparation and quantum state transmission. We find that, like BB84 and E91 protocols, this QKD protocol is secure when the error is below a threshold. In particular, it is more secure than these two QKD protocols, this conclusion is deduced by two different methods. We remark that our result is for general d-dimensional system, and d is prime if the mutually unbiased bases are used.

Before proceed, let us see the original mean king problem. Once upon a time, Alice imposed a deadly challenge for Bob. Initially she owned a qubit, or a spin $\frac{1}{2}$ particle. Then she may measure its angular momentum in x, y or z direction. These choices correspond to these three orthonormal basis: $\{(|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}$, $\{(|0\rangle + i|1\rangle)/\sqrt{2}, (|0\rangle - i|1\rangle)/\sqrt{2}\}$, $\{|0\rangle, |1\rangle\}$. And she kept the result as a secret. After sending the final eigenstate to Bob, she called up Bob and announced the basis she used. Then, Bob was forced to spell out her measurement result immediately, or he was going to be killed.

There exists a miraculous solution giving Bob 100% chance of success. Bob needs to prepare a maximally entangled state between Alice and him in the beginning, $(|00\rangle + |11\rangle)/\sqrt{2}$. Then, after Alice have made the measurement and sent the state back to him, he measures these two particles in a very special basis:

$$
\begin{aligned}
|I(0)\rangle &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}\left(|01\rangle e^{\frac{i\pi}{4}} + |10\rangle e^{-\frac{i\pi}{4}}\right) \\
|I(1)\rangle &= \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{2}\left(|01\rangle e^{\frac{i\pi}{4}} + |10\rangle e^{-\frac{i\pi}{4}}\right) \\
|I(2)\rangle &= \frac{1}{\sqrt{2}}|11\rangle + \frac{1}{2}\left(|01\rangle e^{-\frac{i\pi}{4}} + |10\rangle e^{\frac{i\pi}{4}}\right) \\
|I(3)\rangle &= \frac{1}{\sqrt{2}}|11\rangle - \frac{1}{2}\left(|01\rangle e^{-\frac{i\pi}{4}} + |10\rangle e^{\frac{i\pi}{4}}\right).
\end{aligned}
\tag{312}
$$

Then, using the following table, he could ascertain Alice's result with the basis information.

This fascinating game comes from (Vaidman *et al.*, 1987), even before its name "Mean King" was invented. Then people realized this game can be used as a quantum key distribution protocol(Bub, 2001). Just imagine Alice is not malicious. In fact, she and Bob can use this process as a way to check the safety of this quantum channel. In ideal (noiseless) cases, if there exists an eavesdropper Eve who tries to extract information from this channel, she will inevitably disturb the system and as a consequence, Alice and Bob will find discrepancy in the measurement results.

basis used:	x	y	z
I(0)	$\frac{\lvert 0\rangle+\lvert 1\rangle}{\sqrt{2}}$	$\frac{\lvert 0\rangle+i\lvert 1\rangle}{\sqrt{2}}$	$\lvert 0\rangle$
I(1)	$\frac{\lvert 0\rangle-\lvert 1\rangle}{\sqrt{2}}$	$\frac{\lvert 0\rangle-i\lvert 1\rangle}{\sqrt{2}}$	$\lvert 0\rangle$
I(2)	$\frac{\lvert 0\rangle+\lvert 1\rangle}{\sqrt{2}}$	$\frac{\lvert 0\rangle-i\lvert 1\rangle}{\sqrt{2}}$	$\lvert 1\rangle$
I(3)	$\frac{\lvert 0\rangle-\lvert 1\rangle}{\sqrt{2}}$	$\frac{\lvert 0\rangle+i\lvert 1\rangle}{\sqrt{2}}$	$\lvert 1\rangle$

TABLE I The table of Bob's measurement result, Alice's basis and Alice's measurement result in the 2d Mean King problem

Then they'll get informed of the existence of an invader, hence discard the quantum channel. In (Werner *et al.*, 2009), the security of this protocol in transmission-error-free scenario is proved. Next we will provide a more thorough analysis, displaying the most crucial quantitative result: the maximal allowed error rate(disturbance). Of course, these protocol could be generalized to higher prime dimensional cases (Kimura *et al.*, 2006), and we will also study them.

B. The mean king retrodiction problem as a QKD protocol

Next we study the QKD protocol based on this mean king problem. We start it by considering a d-dimensional system. This quantum retrodiction game is played by Alice and Bob who agree on a Hilbert space $\mathbb{C}$, and a set of orthonormal bases of this space, $|A, a\rangle$, which means a-th basis vector of the A-th bases, the explicit form of it will be given later in Eq.(316). To start the game, Bob first uses a maximally entangled state $\Omega = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$, sends the first particle to Alice and retains the other one. Alice then performs a projective measurement in a bases A at random, keeps both the bases A and the result a secret and returns the particle to Bob. This time, Bob would have a state $|\Phi_{A,a}\rangle = |\overline{A,a}\rangle \otimes |A,a\rangle$, where $|\overline{A,a}\rangle = \sum_{i=0}^{d-1}|i\rangle\langle i|A,a\rangle^*$. Then Bob measures his state, after which Alice announces her bases A, and Bob is required to guess Alice's measurement result a.

Bob's winning strategy has been discussed when Alice exploits mutually unbiased bases (Hayashi *et al.*, 2005; Kimura *et al.*, 2006) as well as in a "meaner" way utilizing biased (nondegenerate) bases (Reimpell and Werner, 2007). Although biased bases may be "meaner" for Eve to guess the right answer in *every single run*, she would probably do better asymptotically by using the correlations between bases to improve the guesses in a long term. As a result, in quantum cryptography, mutually unbiased bases would be a more desirable option, where correlations can be nullified. So, we would focus on the exploitation of mutually unbiased bases from now on.

It is pointed out (Hayashi *et al.*, 2005) that as a winning strategy, Bob should have a guessing function $s(I, A)$ satisfying that

$$\langle \Phi_{A,a}|I\rangle = \frac{1}{\sqrt{d}}\delta_{s(I,A),a}, \tag{313}$$

where $\{|I\rangle\}_{I=0}^{d^2-1}$ are orthonormal measurement base vectors for Bob in Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^d$, and further such $\{|I\rangle\}_{I=0}^{d^2-1}$ may exist if d is a prime. At the same time, there would exist a maximal set of mutually unbiased bases for such d's. The guessing function is explicitly constructed as,

$$s((m,n), A) = \begin{cases} n - Am, \ 0 \leq A \leq d-1, \\ m, \ A = d \end{cases} \tag{314}$$
$$(m, n = 0, 1, 2, \ldots, d-1, \quad I = nd + m),$$

where $n - Am$ should be calculated in the sense of modulo d. So Bob would have such a strategy utilizing his outcome of measurement $|I\rangle$ combined with Alice's announce of her bases A, the guessing function $s(I, A)$ would always provide the result a correctly.

The QKD protocol based on this quantum retrodiction protocol is that Alice and Bob collaborate such that they will share a secrete key a. Note that in the process of the protocol, only the measurement base A is publicly announced.

C. Eavesdropping

The security of the QKD protocol is analyzed by considering a full coherent attack on both quantum channels (Werner *et al.*, 2009), namely Eve controls completely the preparation of entangled pairs, which are used by Bob

before sending one part of them to Alice, as well as the feedback channel which is used for transmitting back the quantum state after a measurement by Alice. To specify the attack, in the former scenario, Eve initially prepares a maximally entangled state $|\Phi^+\rangle_{BB'}$ which will be shared for Alice and Bob. But she adversarial prepares another completely same entangled pair $|\Phi^+\rangle_{EE'}$, partially swaps her qubit with the providing entangled pair. Consequently, Alice and Bob both are partially entangled with Eve, in contrast, they are maximally entangled with each other if no Eve exists. So the whole system with Alice, Bob and Eve possesses a superposition of two pairs maximally entangled states, namely,

$$|\Phi^+\rangle_{BB'}|\Phi^+\rangle_{EE'} \to \sqrt{1-p}|\Phi^+\rangle_{BA}|\Phi^+\rangle_{EE'} + \sqrt{p}|\Phi^+\rangle_{BE}|\Phi^+\rangle_{AE'}, \tag{315}$$

where p is a controllable parameter by Eve so that she can decide the extent of her eavesdropping. For the second channel, Eve is confined to only perform a cloning-based individual attack on the particle Alice sends to Bob after her projective measurement (Bruß, 1998; Cerf, 1998; Cerf *et al.*, 2002a; Xiong *et al.*, 2012).

The set of mutually unbiased bases is formed by the eigenvectors of generalized Pauli matrices in dimension d,

$$\sigma_z, \sigma_x, \sigma_x\sigma_z, \sigma_x\sigma_z^2, \ldots, \sigma_x\sigma_z^{d-1},$$

with $\sigma_x|j\rangle = |j+1\rangle$, $\sigma_z|j\rangle = \omega^j|j\rangle$, and $\omega = e^{i\frac{2\pi}{d}}$. So there are altogether $d+1$ mutually unbiased bases (Bandyopadhyay *et al.*, 2002). We can define, if $d > 2$ is a prime number,

$$|A, a\rangle = \begin{cases} \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\omega^{-a(d-j)-As_j}|j\rangle, \ 0 \le A \le d-1, \\ a, \ A = d, \end{cases} \tag{316}$$

where $s_j = j + \cdots + (d-1)$. Note that the definition differs slightly with (Bandyopadhyay *et al.*, 2002) in sequence without deteriorating their properties. It is explicit that $|A, a\rangle$'s ($0 \le A \le d-1$, $0 \le a \le d-1$) are the eigenvectors of $\sigma_x\sigma_z^A$, and for $A = d$, $0 \le a \le d-1$, $|A, a\rangle$'s are the eigenvectors of σ_z. We also know

$$\langle a_0|A, a\rangle = \frac{1}{\sqrt{d}}\left(\omega^{-a}\right)^{d-a_0}\left(\omega^{-A}\right)^{s_{a_0}}. \tag{317}$$

For $d = 2$, the expressions of the bases are different. As we have already reviewed, the sets of states are in (312).

With the whole system in the form of Eq.(315), Alice and Bob run the agreed QKD protocol as planned as if no Eve existing. Alice performs a projective measurement by a base randomly chosen from a *subset* of the $d+1$ mutually unbiased bases, for example $g+1$ of them ($1 \le g \le d$). Her state will then collapse to $|A_0, a_0\rangle$, and be sent to Bob through a quantum channel controlled by Eve. Alice keeps the measurement result a_0 and the base A_0 secret first, but announces A_0 later after Bob receives the sending state. When $|A_0, a_0\rangle$ is sent by Alice, Eve will generally use the attack based on the scheme of quantum cloning (Bruß, 1998; Cerf, 1998). For case of $g+1$ mutually unbiased bases, the scheme of quantum cloning attack is presented in (Xiong *et al.*, 2012).

Namely, when Alice returns the particle $|A_0, a_0\rangle$ through a quantum channel controlled by Eve, Eve can attack it by an asymmetric cloning, yielding,

$$\begin{aligned} U|A, a\rangle_B|\Phi_{00}\rangle_{E'E} &= \sum_{m,n} a_{mn}U_{m,n}|A, a\rangle_A \otimes |\Phi_{-m,n}\rangle_{E'E} \\ &= \sum_{m,n} b_{mn}|\Phi_{-m,n}\rangle_{AE'} \otimes U_{m,n}|A, a\rangle_E, \end{aligned} \tag{318}$$

with $\sum_{m,n}|a_{mn}|^2 = 1$, $b_{mn} = \frac{1}{d}\sum_{k,r}a_{kr}\omega^{kn-rm}$, and $U_{m,n} = \sigma_x^m\sigma_z^n$. We can use the following notations (Xiong *et al.*, 2012),

$$a_{mn} = \begin{cases} v, \ m = n = 0, \\ x, \ m = 0, n \neq 0 \text{ or } m \neq 0, n = km, \\ y, \ \text{ otherwise}, \end{cases} \tag{319}$$

where $k = 0, ..., g-1$, and v is a real number to be determined.

By tracing out E and E', we discover that the density operator for Bob would be

$$\begin{aligned} \rho_{Bob} = &\left[(1-p)|\overline{A_0, a_0}\rangle\langle\overline{A_0, a_0}| + p\frac{\mathbb{I}}{d}\right] \otimes \Bigg\{ \left[v^2 + (d-1)x^2\right]|A_0, a_0\rangle\langle A_0, a_0| \\ &+ \sum_{j=1}^{d-1}\left[gx^2 + (d-g)y^2\right]|A_0, a_0 + j\rangle\langle A_0, a_0 + j| \Bigg\}. \end{aligned} \tag{320}$$

Note the second part has already been attacked by Eve through a quantum cloning, and v, x and y are parameters controlled by Eve so that she may optimize her attack.

Similarly, the density operator of Eve takes the form,

$$\begin{aligned}\rho_{Eve} &= \left[p|\overline{A_0,a_0}\rangle\langle\overline{A_0,a_0}| + (1-p)\frac{\mathbb{I}}{d}\right] \otimes \left\{ \left[v'^2 + (d-1)x'^2\right] |A_0,a_0\rangle\langle A_0,a_0| \right. \\ &\left. + \left[gx'^2 + (d-g)y'^2\right] \times \times \sum_{j=1}^{d-1} |A_0,a_0+j\rangle\langle A_0,a_0+j| \right\}. \end{aligned} \tag{321}$$

Without knowing Eve's attack, Bob would simply measure the states in bases $\{|I\rangle\}_{I=0}^{d^2-1}$ as if no disturbance has been introduced in the system. Bob's fidelity is defined as his possibility to obtain the right result a_0, namely

$$F_{Bob} = \sum_{I=0}^{d^2-1} \delta_{s(I,A_0),a_0} \langle I|\rho_{Bob}|I\rangle. \tag{322}$$

Eve can use completely similar measurement to find the correct variable a_0, and the possibility is quantified by her fidelity.

D. Fidelities of Bob and Eve

Next we try to find the analytic result of the fidelities. For $d = 2$, suppose $A_0 = 0, a_0 = 0$ without lose of generality, then we have,

$$\begin{aligned}\rho_{Bob} &= \left[\left(1-\frac{p}{2}\right)|0\rangle\langle 0| + \frac{p}{2}|1\rangle\langle 1|\right] \otimes \{(v^2+x^2)|0\rangle\langle 0| + [gx^2 + (2-g)y^2]|1\rangle\langle 1|\}, \\ \rho_{Eve} &= \left(\frac{1+p}{2}|0\rangle\langle 0| + \frac{1-p}{2}|1\rangle\langle 1|\right) \otimes \{(v'^2+x'^2)|0\rangle\langle 0| + [gx'^2 + (2-g)y'^2]|1\rangle\langle 1|\}. \end{aligned} \tag{323}$$

Fidelities of Bob and Eve can therefore be explicitly calculated as,

$$\begin{aligned}F_{Bob} &= \frac{1}{2} - \frac{p}{4} + \frac{1}{2}(v^2+x^2) \\ F_{Eve} &= \frac{1+p}{4} + \frac{1}{2}(v'^2+x'^2). \end{aligned} \tag{324}$$

For $d > 2$ cases, we introduce the notations, $|\Psi_{A,a}^{(j)}\rangle = |\overline{A,a}\rangle \otimes |A,a+j\rangle (j \neq 0)$, and $|\Phi_{A,a}\rangle = |\overline{A,a}\rangle \otimes |A,a\rangle$.

Use similar method as discussed in (Hayashi *et al.*, 2005), we can show that this set Φ consisting of $d(d+1)$ states $\{|\Phi_{A,a}\rangle\}_{A=0,a=0}^{A=d,a=d-1}$, is complete in the composite space $\mathbb{C}^d \otimes \mathbb{C}^d$, as presented below. Suppose a linear relation with some coefficients $c_{A,a}$ holds:

$$\sum_{A,a} c_{A,a}|\Phi_{A,a}\rangle = 0. \tag{325}$$

Multiplying bra vector $\langle\Phi_{A',a'}|$ from the left and we immediately obtain,

$$c_{A',a'} + \sum_{A\neq A'} \frac{1}{d} \sum_a c_{A,a} = 0, \tag{326}$$

which implies that the coefficient $c_{A,a}$ should be independent of a. We have made use of the equation,

$$\langle\Phi_{A',a}|\Phi_{A,a}\rangle = \delta_{AA'}\delta_{aa'} + \frac{1-\delta_{AA'}}{d}. \tag{327}$$

Now consider a subset Φ'_{A_0,a_0} which consists of d^2 states obtained by removing d states $\{|\Phi_{A,a}\rangle\}_{A\neq A_0, a=s(I_0,A)}$ from Φ, where I_0 is defined as arbitrary I satisfying $\delta_{a_0,s(I,A_0)} = 1$. The above equations still hold for Φ'_{A_0,a_0}. Since $c_{A,s(I_0,A)} = 0$ for $A \neq A_0$, we would have $c_{A,a} = 0$ for all $A \neq A_0$. And for $A = A_0$, we would have,

$$\sum_a c_{A_0,a}|\Phi_{A_0,a}\rangle = 0. \tag{328}$$

Since $|\Phi_{A_0,a}\rangle$ are a set of orthogonal bases, we would have $c_{A_0,a} = 0$. Thus the d^2 states in Φ'_{A_0,a_0} are linearly independent and the set Φ is complete in the d^2-dimensional composite space $\mathbb{C}^d \otimes \mathbb{C}^d$.

As a result, $|\Psi^{(j)}_{A_0,a_0+k}\rangle$ can be represented in a unique way as the linear combination of the states consisted in Φ'_{A_0,a_0}. And we would use Gram-Schmidt orthogonal-normalization process to obtain the orthonormal basis in $\mathbb{C}^d \otimes \mathbb{C}^d$ first. It is obvious that

$$\langle \Phi_{A_0,a} | \Phi_{A_0,a'} \rangle = \delta_{aa'}. \tag{329}$$

So the first d basis, $|\Phi_{A_0,a}\rangle_{a=0}^{d-1}$ has already been orthogonalized as well as normalized. For other basis, now we consider the set $|\Phi_{A,s(I_0,A)+1+i}\rangle_{i=0}^{d-2}$ for $A \neq A_0$(note that modular d is always omitted for convenience), and we have,

$$\langle \Phi_{A_0,a} | \Phi_{A,s(I_0,A)+1+i} \rangle = \frac{1}{d}. \tag{330}$$

So for $i = 0$, the orthogonalized base would be,

$$|\psi_{A,s(I_0,A)+1}\rangle = |\Phi_{A,s(I_0,A)+1}\rangle - \frac{1}{d}\sum_{a=0}^{d-1} |\Phi_{A_0,a}\rangle. \tag{331}$$

Taken into account that $|\Phi\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle = \frac{1}{\sqrt{d}}\sum_{a=0}^{d-1}|\Phi_{A,a}\rangle$ for arbitrary A's, we can conclude that $\sum_{a=0}^{d-1}|\Phi_{A_0,a}\rangle = \sum_{i=0}^{d-1}|\Phi_{A,s(I_0,A)+1+i}\rangle$, and $\langle\psi_{A,s(I_0,A)+1}|\psi_{A,s(I_0,A)+1}\rangle = \frac{(d-1)^2}{d^2} + (d-1)\frac{1}{d^2} = \frac{d-1}{d}$. So we have generated another orthonormal base,

$$|\phi_{A,s(I_0,A)+1}\rangle = \sqrt{\frac{d}{d-1}}\left[|\Phi_{A,s(I_0,A)+1}\rangle - \frac{1}{d}\sum_{i=0}^{d-1}|\Phi_{A,s(I_0,A)+1+i}\rangle\right]. \tag{332}$$

And for $i = 1$, since $\langle\phi_{A,s(I_0,A)+1}|\Phi_{A,s(I_0,A)+1+1}\rangle = -\frac{1}{d}\sqrt{\frac{d}{d-1}}$, the orthogonalized base is,

$$|\psi_{A,s(I_0,A)+1+1}\rangle = |\Phi_{A,s(I_0,A)+1+1}\rangle - \frac{1}{d}\sum_{i=0}^{d-1}|\Phi_{A,s(I_0,A)+1+i}\rangle + \frac{1}{d}\sqrt{\frac{d}{d-1}}|\phi_{A,s(I_0,A)+1}\rangle. \tag{333}$$

Furthermore, we can calculate the corresponding normalized base,

$$|\phi_{A,s(I_0,A)+1+1}\rangle = \sqrt{\frac{d-1}{d-2}}[|\Phi_{A,s(I_0,A)+1+1}\rangle - \frac{1}{d-1}\sum_{j=i}^{d-1}|\Phi_{A,s(I_0,A)+1+i}\rangle]. \tag{334}$$

By repeating the procedures above, we can figure out all the orthonormal basis are $|\Phi_{A_0,a}\rangle_{a=0}^{d-1}$ and $|\phi_{A,s(I_0,A)+1+i}\rangle_{i=0}^{d-2}$(for the latter set, $A \neq A_0$), where

$$\begin{cases} |\Phi_{A_0,a}\rangle = |\overline{A_0,a}\rangle \otimes |A_0,a\rangle, \\ |\phi_{A,s(I_0,A)+1+i}\rangle = \sqrt{\frac{d-i}{d-i-1}}\left[|\Phi_{A,s(I_0,A)+1+i}\rangle - \frac{1}{d-i}\sum_{k=i}^{d-1}|\Phi_{A,s(I_0,A)+1+k}\rangle\right]. \end{cases} \tag{335}$$

Since the sets of MUBs can be related by a unitary transform, we can, for convenience, define $A_0 = d+1$, without loss of generality. So $|\Psi^{(j)}_{A_0,a_0+k}\rangle = |a_0+k+j\rangle \otimes |a_0+k\rangle$. And as the property of MUB requires,

$$\langle A_0, a_0 | A, a\rangle = \frac{1}{\sqrt{d}}\left(\omega^{-a}\right)^{d-a_0}\left(\omega^{-A}\right)^{s_{a_0}}. \tag{336}$$

Here $\omega = \exp\{i\frac{2\pi}{d}\}$.

For $A \neq A_0$,

$$\begin{aligned} \langle\Phi_{A,a}|\Psi^{(j)}_{A_0,a_0+k}\rangle &= \langle\overline{A,a}|\overline{A_0,a_0+k}\rangle\langle A,a|A_0,a_0+k+j\rangle \\ &= \langle A_0,a_0+k|A,a\rangle\langle A,a|A_0,a_0+k+j\rangle \\ &= \frac{1}{d}\left(\omega^{-a}\right)^d\left(\omega^{-A}\right)^{s_{a_0+k}}\left(\omega^{a}\right)^{d-j}\left(\omega^{A}\right)^{s_{a_0+k+j}} \\ &= \frac{1}{d}\omega^{-j\left[a+\frac{A}{2}(2a_0+2k+j-1)\right]}. \end{aligned} \tag{337}$$

$$\tag{338}$$

As a result,

$$\begin{aligned}\langle \phi_{A,s(I_0,A)+1+i}|\Psi^{(j)}_{A_0,a_0+k}\rangle &= \frac{1}{d}\omega^{-j(s(I_0,A)+1)-\frac{A}{2}j(2a_0+2k+j-1)} \\ &\quad\times\sqrt{\frac{d-i}{d-i-1}}\left[\omega^{-ji}-\frac{1}{d-i}\sum_{k=i}^{d-1}\omega^{-jk}\right],\end{aligned} \tag{339}$$

and

$$\langle \Phi_{A_0,a}|\Psi^{(j)}_{A_0,a_0+k}\rangle = 0. \tag{340}$$

Now we can explicitly represent $|\Psi^{(j)}_{A_0,a_0+k}\rangle$ in the orthonormal basis we constructed before.
And further, for $j \neq 0$, we have

$$\begin{aligned}|\Psi^{(j)}_{A_0,a_0+k}\rangle &= \sum_{A=0}^{d-1}\sum_{i=0}^{d-2}\frac{1}{d}\frac{d-i}{d-i-1}\omega^{A\left(s_{a_0+k+j}-s_{a_0+k}\right)-j(s(I_0,A)+1)} \\ &\quad\times\left(\omega^{-ij}-\frac{1}{d-i}\sum_{l=i}^{d-1}\omega^{-lj}\right)|\phi_{A,s(I_0,A)+1+i}\rangle\end{aligned} \tag{341}$$

Taking into account that $\langle I|\Phi_{A,a}\rangle = \frac{1}{\sqrt{d}}\delta_{s(I,A),a}$, we would have,

$$\begin{aligned}\langle I_0|\Psi^{(j)}_{A_0,a_0+k}\rangle &= \frac{1}{\sqrt{d}}\sum_{i=0}^{d-2}\frac{1}{d}\frac{d-i}{d-i-1}\omega^{A\left(s_{a_0+k+j}-s_{a_0+k}\right)-j(s(I_0,A)+1)} \\ &\quad(\omega^{-ij}-\frac{1}{d-i}\sum_{l=i}^{d-1}\omega^{-lj})\left(-\frac{1}{d-i}\right) \\ &= \sum_{A=0}^{d-1}\frac{1}{d^{3/2}}\omega^{A\left(s_{a_0+k+j}-s_{a_0+k}\right)-js(I_0,A)} \\ &= \sum_{A=0}^{d-1}\frac{1}{d^{3/2}}\omega^{-nj}\omega^{Aj(2k+j-1)/2}.\end{aligned} \tag{342}$$

If $j \neq 1-2k$, we would have $\langle I_0|\Psi^{(j)}_{A_0,a_0+k}\rangle = 0$. Otherwise, $\langle I_0|\Psi^{(j)}_{A_0,a_0+k}\rangle = \frac{1}{\sqrt{d}}\omega^{-nj}$, n is decided by I_0.
The density operator for Bob would be

$$\begin{aligned}\rho_{Bob} &= \left[(1-p)|\overline{A_0,a_0}\rangle\langle\overline{A_0,a_0}| + p\frac{\mathbb{I}}{d}\right]\otimes\Bigg\{\left[v^2+(d-1)x^2\right]|A_0,a_0\rangle\langle A_0,a_0| \\ &+ \sum_{j=1}^{d-1}\left[gx^2+(d-g)y^2\right]|A_0,a_0+j\rangle\langle A_0,a_0+j|\Bigg\}.\end{aligned} \tag{343}$$

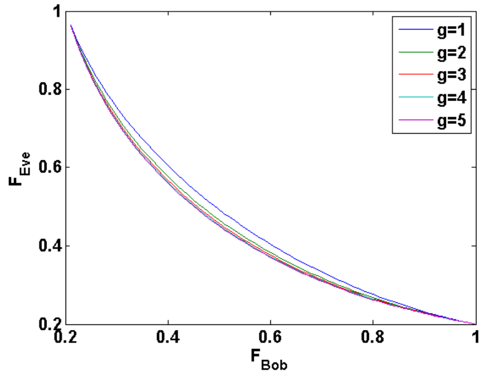


FIG. 9 (color online) F_{Eve} - F_{Bob} curve for various g's when $d = 5$. The curves are numerically calculated from Eq.(344) and Eq.(346).

using (322),

$$
\begin{aligned}
F_{Bob} \;=\; & \sum_{I_0=0}^{d^2-1} \delta_{s(I_0,A_0),a_0} \Bigg\{ (1-p)\left[v^2+(d-1)x^2\right] \langle I_0|\Phi_{A_0,a_0}\rangle\langle\Phi_{A_0,a_0}|I_0\rangle \\
& +(1-p)\left[gx^2+(d-g)y^2\right] \sum_{j=1}^{d-1} \langle I_0|\Psi^{(j)}_{A_0,a_0}\rangle\langle\Psi^{(j)}_{A_0,a_0}|I_0\rangle \\
& +\frac{p}{d}\left[v^2+(d-1)x^2\right] \sum_{k=0}^{d-1} \langle I_0|\Psi^{(-k)}_{A_0,a_0+k}\rangle\langle\Psi^{(-k)}_{A_0,a_0+k}|I_0\rangle \\
& +\frac{p}{d}\left[gx^2+(d-g)y^2\right] \sum_{k=0}^{d-1}\sum_{j=1}^{d-1} \langle I_0|\Psi^{(j-k)}_{A_0,a_0+k}\rangle\langle\Psi^{(j-k)}_{A_0,a_0+k}|I_0\rangle \Bigg\} \\
=\; & (1-p)\left[v^2+(d-1)x^2\right] + (1-p)\left[gx^2+(d-g)y^2\right] \\
& +\frac{p}{d}\left[v^2+(d-1)x^2\right] + (d-1)\frac{p}{d}\left[gx^2+(d-g)y^2\right] \\
=\; & (1-p)\left[v^2+(d+g-1)x^2+(d-g)y^2\right] + \frac{p}{d}.
\end{aligned} \tag{344}
$$

We have already used the equation $\sum_{I=0}^{d^2-1} \delta_{s(I,A),a} |\langle I|\Phi_{A,a}\rangle|^2 = 1$

Similarly, we can have Eve's density operator,

$$
\begin{aligned}
\rho_{Eve} \;=\; & \left[p|\overline{A_0,a_0}\rangle\langle\overline{A_0,a_0}| + (1-p)\frac{\mathbb{I}}{d}\right] \\
& \otimes \left\{ \left[v'^2+(d-1)x'^2\right] |A_0,a_0\rangle\langle A_0,a_0| + \left[gx'^2+(d-g)y'^2\right] \sum_{j=1}^{d-1} |A_0,a_0+j\rangle\langle A_0,a_0+j| \right\}
\end{aligned} \tag{345}
$$

If Eve adopts the same protocol as Bob does, her fidelity would be,

$$
F_{Eve} \;=\; \frac{1-p}{d} + p\left[v'^2+(d+g-1)x'^2+(d-g)y'^2\right]. \tag{346}
$$

To visually represent the performance of Eve, we choose $d = 5$ as an example and plot optimized F_{Eve} (by tuning both p and v in the two quantum channels) as a function of F_{Bob} in FIG.9. With increasing F_{Bob}, F_{Eve} diminishes, which coincides with intuition that with more disturbance, Eve gets more information while Bob loses more. Also, with the increase of g, security will be improved.

This result is similar with standard QKD protocols as studied in (Bruß, 1998; Cerf *et al.*, 2002a; Gisin *et al.*, 2002; Xiong *et al.*, 2012). In cases where Bob's fidelity is larger than that of Eve, the protocol is assumed to be secure. Moreover, we will show explicitly later that the retrodiction QKD protocol has a higher security.

E. Security analysis by mutual information in mean king QKD

A QKD protocol is secure when mutual information between Alice and Bob is larger than that between Alice and Eve, under this condition can Alice and Bob use classical error correction and privacy amplification methods (Cerf *et al.*, 2002a; Gisin *et al.*, 2002) to guarantee a secure communication. In the retrodiction QKD scheme, Alice sends each state in A_0 with probability $\frac{1}{d}$, and Bob would obtain the right result a_0 with probability F_{Bob}.

First, we can explicitly write the final states of quantum states associated with Bob and Eve as,

$$\left(\frac{1}{\sqrt{d}}|i\rangle_{B_1}|i\rangle_{E_1}|i\rangle_{E_1'}+\sqrt{1-p}|i\rangle_{B_1}\sum_{a'\neq i}\frac{1}{\sqrt{d}}|a'\rangle_{E_1}|a'\rangle_{E_1'}+\sqrt{p}\sum_{a'\neq i}\frac{1}{\sqrt{d}}|a'\rangle_{B_1}|a'\rangle_{E_1}|i\rangle_{E_1'}\right)$$
$$\otimes\sum_{m,j}\left(\frac{1}{\sqrt{d}}\sum_n a_{mn}\omega^{n(i-j)}\right)|i+m\rangle_{B_2}|j\rangle_{E_2}|j+m\rangle_{E_2'}. \tag{347}$$

As the calculation in (Xiong *et al.*, 2012), we have,

$$\begin{aligned} I_{AB} &= -\sum_{a_1,a_2}p(a_1,a_2)\log_2 p(a_1,a_2) \\ &\quad +\sum_{i,a_1,a_2}p(i)p(a_1,a_2|i)\log_2 p(a_1,a_2|i), \end{aligned}$$

$$\begin{aligned} I_{AE} &= -\sum_{e_1,e_1',e_2,e_2'}p(e_1,e_1',e_2,e_2')\log_2 p(e_1,e_1',e_2,e_2') \\ &\quad +\sum_{i,e_1,e_1',e_2,e_2'}p(i)p(e_1,e_1',e_2,e_2'|i)\log_2 p(e_1,e_1',e_2,e_2'|i), \end{aligned}$$

Assume that Alice measures her states randomly, so $p(i)=\frac{1}{d}$ for arbitrary i. Thus,

$$\begin{aligned} p(a_1,a_2) &= \frac{1}{d}\sum_i p(a_1,a_2|i), \\ p(e_1,e_1',e_2,e_2') &= \frac{1}{d}\sum_i p(e_1,e_1',e_2,e_2'|i). \end{aligned}$$

And we can further deduce that a_1 and a_2 are independent, and e_1, e_1' are independent on e_2 and e_2', which is due to the uncorrelation of two quantum channels when Eve attacks. As a result,

$$\begin{aligned} p(a_1,a_2|i) &= p(a_1|i)\cdot p(a_2|i), \\ p(e_1,e_1',e_2,e_2'|i) &= p(e_1,e_1'|i)\cdot p(e_2,e_2'|i). \end{aligned}$$

In addition, we have the following considerations,

$$\begin{aligned} p(a_1|i) &= \begin{cases}\frac{1}{d}+\frac{d-1}{d}(1-p), & a_1=i,\\ \frac{p}{d}, & a_1\neq i.\end{cases} \\ p(a_2|i) &= \begin{cases}v^2+(d-1)x^2, & a_2=i,\\ gx^2+(d-g)y^2, & a_2\neq i.\end{cases} \\ p(e_1,e_1'|i) &= \begin{cases}\frac{1}{d}, & e_1=e_1'=i,\\ \frac{1-p}{d}, & e_1=e_1'\neq i,\\ \frac{p}{d}, & e_1'=i, e_1\neq i,\\ 0, & e_1'\neq i, e_1\neq e_1'.\end{cases} \\ p(e_2,e_2'|i) &= \begin{cases}\frac{[v+(d-1)x]^2}{d}, & e_2=e_2'=i,\\ \frac{(v-x)^2}{d}, & e_2=e_2'\neq i,\\ \frac{[gx+(d-g)y]^2}{d}, & e_2'=i, e_2\neq i,\\ \frac{(x-y)^2}{d}\left|\frac{1-\omega^{mg(i-e_2')}}{1-\omega^{m(i-e_2')}}\right|^2, & e_2'\neq i, e_2\neq e_2'.\end{cases} \end{aligned}$$

To analyze the security of this protocol, we have two different definition of disturbance: D_I and D_F, as explained in (Xiong *et al.*, 2012). Here D_I is defined by optimizing parameters p, v so that maximized $I_{AE} - I_{AB}$ is obtained with a certain F_{Bob}. Then we can obtain a critical F^*_{Bob}, where $\max\{I_{AE} - I_{AB}\} = 0$, and D_I is defined as $1 - F^*_{Bob}$. But for D_F, as in (Cerf *et al.*, 2002a), we fix parameters p, v for a given F_{Bob} when maximal F_{Eve} is obtained. Then F^*_{Bob} is defined by $I_{AE} - I_{AB} = 0$, and its corresponding disturbance $D_F = 1 - F^*_{Bob}$. These two definitions may lead to different results, as shown in (Xiong *et al.*, 2012). Since we hope to directly analyze mutual information, adopting D_I as the index of disturbance is more appropriate. In this scenario, the protocol is secure if and only if Bob's fidelity is larger than $1 - D_I$. Some numerical results are in TABLE II.

	d	g = 1	2	3	4	5	6	7
$D_I(\%)$	2	15.64	16.62					
	3	22.92	24.31	24.57				
	5	39.72	41.27	41.51	41.60	41.65		
	7	46.88	48.05	48.20	48.27	48.31	48.33	48.34

TABLE II Disturbance D_I associated with maximal $I_{AE} - I_{AB}$. Corresponding parameters p and v are optimized, and $D_I = 1 - F^*_{Bob}$, where F^*_{Bob} is Bob's fidelity with $\max\{I_{AE} - I_{AB}\} = 0$. When $F_{Bob} > 1 - D_I$, Bob and Alice can use classical methods to reduce exponentially small Eve's information.

F. The retrodiction QKD is more secure than BB84 and six-state protocols

For $d = 2$, we have the fidelity expressions (324). And for fixed F_{Bob}, we can choose parameters v and p to maximize F_{Eve}. And from previous results (Xiong *et al.*, 2012), we have, for BB84 protocol, $F_{Eve} = \frac{1}{2}\left(\sqrt{F_{Bob}} + \sqrt{1 - F_{Bob}}\right)^2$, and for six-state protocol, $F_{Eve} = \left(\sqrt{3F_{Bob} - 1} + \sqrt{1 - F_{Bob}}\right)^2 / \sqrt{8} + (1 - F_{Bob})$. These four cases are illustrated in FIG.10. Interestingly, it is clear that the retrodiction QKD protocol presented here is more secure than BB84 protocol and six-state protocol, i.e., with fixed disturbance (F_{Bob} is fixed), Eve's probability to figure out the correct result is lower. And using 3 bases ($g = 2$) is even more secure than 2 bases($g = 1$). This conclusion can be confirmed by comparing numerical results of traditional QKD(explicitly shown in TABLE III) with our results.

	d	g = 1	2	3	4	5	6	7
$D_I(\%)$	2	14.64	15.64					
	3	21.13	22.47	22.67				
	5	27.60	28.91	29.12	29.20	29.23		
	7	30.90	32.10	32.26	32.32	32.36	32.38	32.39

TABLE III Disturbance D_I in (Xiong *et al.*, 2012). Every entry is exactly smaller than corresponding ones in mean king retrodiction protocol.

G. Discussions about mean king problem

In summary, we have explicitly shown that the mean king retrodiction QKD protocol, like standard QKDs such as BB84 and E91, is unconditional secure. Its security is analyzed by considering attacks on both the entangled pair preparation and quantum state transmission. Interestingly, this QKD protocol has a higher security than the corresponding standard QKD in the sense that it tolerates higher error rate. Our security analysis is based on two methods, comparison of fidelities for Bob and Eve, and comparison of mutual information. This security proof can be extended to completely coherent attack by considering multipartite scheme, which is similar as standard QKD.

By considering the efficiency of the mean king retrodiction QKD, one can find that it has the advantage of generating a raw key in *every single run* no matter how many mutually unbiased bases are utilized. For comparison, in standard QKD by exploiting $g + 1$ mutually unbiased bases, there would only have a raw key in $g + 1$ runs on average for Alice and Bob. Of course, if quantum memory is available, it can also have a high efficiency in generating raw keys. However, the current quantum memory has limited storage time, it is still possible that the retrodiction QKD protocol needs short-time memory since no announcement of bases is necessary for the measurement of Bob, this is quite different with the standard QKD.

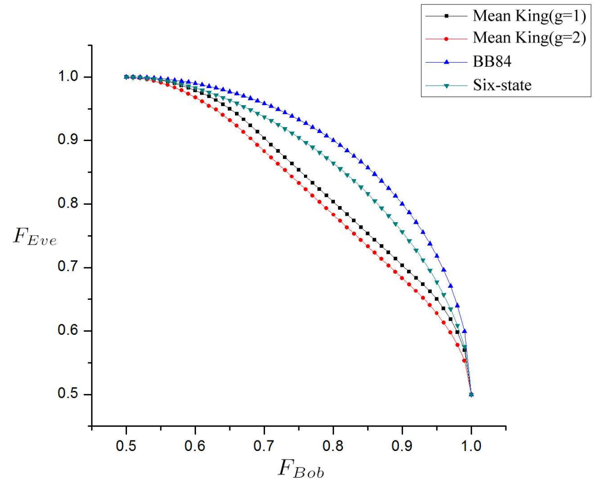


FIG. 10 (color online) F_{Eve} vs F_{Bob} curve for $d = 2$. In our scenario, the mean king retrodiction QKD has higher security than both BB84 and six-state protocols.

The BB84 QKD protocol is almost commercialized. As generally accepted, there is no doubt that the protocol itself is secure, however practically, its security relies significantly on physical implementations. So it is still of great interest if we can have a simple but more secure QKD protocol. As we have shown that retrodiction QKD protocol is more secure, and it can generate a raw key in every single run, it is hopeful that it can open a new direction for a practical QKD implementation.

X. SEQUENTIAL UNIVERSAL QUANTUM CLONING

In past years, theoretical research on quantum cloning machines have progressed greatly. At the same time, experimentally various cloning schemes have been realized, by using polarized photons(Irvine *et al.*, 2004; Lamas-Linares *et al.*, 2002; Pelliccia *et al.*, 2003; Ricci *et al.*, 2004) or nuclear spins in NMR (Cummins *et al.*, 2002; Du *et al.*, 2005). However, these experiments are only restricted to $1 \to 2$ or $1 \to 3$ cloning machines, leaving the general case of $N \to M$ cloning unsolved. The difficulty of realizing $N \to M$ cloning mainly arises in preparing multipartite entangled states, since it is very difficult to perform a global unitary operation on large-dimensional systems to create multipartite entangled states. While on the other hand, using the technique of sequential cloning, one may be able to divide the big global unitary operation into small ones, each of which is only concerned with a small quantum system and as a result makes it possible to get the desired entangled state. Several quantum cloning procedures for multipartite cloning were proposed, but they are not in the sequential method(Fan *et al.*, 2003; Simon *et al.*, 2000). In 2007, based on the work of Vidal (Vidal, 2003), Delgado *et al.* proposed a scheme of a sequential $1 \to M$ cloning machine(Delgado *et al.*, 2007). Since the procedure is sequential, it significantly reduces the difficulty of its realization. Later, Dang and Fan came up with a scheme which makes the more general $N \to M$ sequential cloning possible (Dang and Fan, 2008). The case of $N \to M$ sequential cloning of qudits is also proposed briefly, yet the details are not presented. The essential idea of sequential method is to express the desired state in the form of matrix product state (MPS), and according to results in (Schon *et al.*, 2005), any MPS can be sequentially generated. On the other hand, it is also pointed out that sequential unitary decompositions are not always successful for genuine entangling operations (Lamata *et al.*, 2008). Here in this section, we will present in detail how the procedure of $1 \to M$ and $N \to M$ sequential cloning works.

A. $1 \to M$ sequential UQCM

According to the method of Delgado *et al.*(Delgado *et al.*, 2007), we first need an ancilla system of dimension D. Let $\mathcal{H}_{\mathcal{A}}$ denotes the D-dimensional Hilbert space of the ancilla system, and $\mathcal{H}_{\mathcal{B}}$ the 2-dimensional Hilbert space of one qubit. In every step of the sequential cloning, we perform a quantum evolutional operator V on the product space of the ancilla and a single qubit. Here we suppose that each qubit is initially state $|0\rangle$ which will not appear in the following equations. V then can be represented by an isometric transformation: $V : \mathcal{H}_{\mathcal{A}} \to \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$, in which $V = \sum_{i,\alpha,\beta} V^i_{\alpha,\beta} |\alpha, i\rangle\langle\beta|$. Let $V^i = \sum_{\alpha,\beta} V^i_{\alpha,\beta}|\alpha\rangle\langle\beta|$, then V^i is a $D \times D$ matrix and satisfies the isometry condition $\sum_i V^{i\dagger} V^i = I$. Let the initial state of the ancilla be $|\phi_I\rangle \in \mathcal{H}_{\mathcal{A}}$. We make the ancilla to interact with the qubits once a time and sequentially, after the unitary operation, we would not recover the ancilla state. So when n operations have been done, the final output state of the ancilla and all the qubits take the form, $|\Psi\rangle = V^{[n]}...V^{[2]}V^{[1]}|\phi_I\rangle$, where indices in squared brackets represent the steps of sequential generation. Now we need to decouple the aniclla from the multi-entangled qubits, and then the n-qubit state shall be left:

$$|\psi\rangle = \sum_{i_1,i_2,...,i_n} \langle\phi_F|V^{[n]i_n}...V^{[1]i_1}|\phi_I\rangle|i_1...i_n\rangle, \tag{348}$$

where ϕ_F represents the final state of the ancilla. For 2-dimensional system $\{|0\rangle, |1\rangle\}$, the cloning transformation of the optimal $1 \to M$ cloning machine is (Gisin and Massar, 1997):

$$|0\rangle \otimes |R\rangle \to |\Psi^{(0)}_M\rangle = \sum_{j=0}^{M-1} \beta_j |(M-j)0, j1\rangle \otimes |(M-j-1)1, j0\rangle_R, \tag{349}$$

$$|1\rangle \otimes |R\rangle \to |\Psi^{(1)}_M\rangle = \sum_{j=0}^{M-1} \beta_{M-j-1} |(M-j-1)0, (j+1)1\rangle \otimes |(M-j-1)1, j0\rangle_R, \tag{350}$$

in which $\beta_j = \sqrt{2(M-j)/M(M+1)}$, $|(M-j-1)1, j0\rangle_R$ is the final state of the cloning machine, and $|(M-j)0, j1\rangle$ denotes the normalized completely symmetric M-qubit state with $(M-j)$ qubits in $|0\rangle$ and j qubits in $|1\rangle$. In order to clone a general state $|\phi\rangle$, it is necessary to know how to sequentially generate the states $|\Psi^{(0)}_M\rangle$ and $|\Psi^{(1)}_M\rangle$, as a result of which we need to express these two states in the MPS form:

$$|\Psi^{(0)}_M\rangle = \sum_{i_1,...i_n} \langle\phi^{(0)}_F|V_0^{[n]i_n}...V_0^{[1]i_1}|0\rangle_D|i_1...i_n\rangle, \tag{351}$$

$$|\Psi^{(1)}_M\rangle = \sum_{i_1,...i_n} \langle\phi^{(1)}_F|V_1^{[n]i_n}...V_1^{[1]i_1}|0\rangle_D|i_1...i_n\rangle. \tag{352}$$

Now we aim to get the explicit expression of the matrices $V_0^{[k]i_k}$ and $V_1^{[k]i_k}$. A way to do so is by using Schmidt decomposition(SD) (Vidal, 2003), see textbook (Nielsen and Chuang, 2000). Consider an arbitrary state $|\Psi\rangle$ in Hilbert space $\mathcal{H}_2^{\otimes n}$, the SD of $|\Psi\rangle$ according to the bipartition $A : B$ is

$$|\Psi\rangle = \sum_{\alpha} \lambda_\alpha |\Phi_\alpha^{[A]}\rangle |\phi_\alpha^{[B]}\rangle, \tag{353}$$

where $|\Phi_\alpha^{[A]}\rangle(|\Phi_\alpha^{[B]}\rangle)$ is an eigenvector of the reduced density matrix $\rho^{[A]}(\rho^{[B]})$ with eigenvalue $|\lambda_\alpha|^2 \geq 0$, and the Schmidt coefficient λ_α satisfies $\langle\Phi_\alpha^{[A]}|\Psi\rangle = \lambda_\alpha|\Phi_\alpha^{[B]}\rangle$.

With the help of SD, we proceed the following protocol:

1. Compute the SD of $|\Psi\rangle$ according to the bipartite $1 : n-1$ splitting of the n-qubit system, which is

$$|\Psi\rangle = \sum_{\alpha_1} \lambda_{\alpha_1}^{[1]} |\Phi_{\alpha_1}^{[1]}\rangle |\Phi_{\alpha_1}^{[2\ldots n]}\rangle \tag{354}$$

$$= \sum_{i_1,\alpha_1} \Gamma_{\alpha_1}^{[1]i_1} \lambda_{\alpha_1}^{[1]} |i_1\rangle |\Phi_{\alpha_1}^{[2\ldots n]}\rangle, \tag{355}$$

   where in the second line we have expressed the Schmidt vector $|\Phi_{\alpha_1}^{[1]}\rangle$ in the computational basis $\{|0\rangle, |1\rangle\}$: $|\Phi_{\alpha_1}^{[1]}\rangle = \sum_{i_1} \Gamma_{\alpha_1}^{[1]i_1}|i_1\rangle$.

2. Expand $|\Phi_{\alpha_1}^{[2\ldots n]}\rangle$ in local basis for qubit 2,

$$|\Phi_{\alpha_1}^{[2\ldots n]}\rangle = \sum_{i_2} |i_2\rangle |\tau_{\alpha_1 i_2}^{[3\ldots n]}\rangle. \tag{356}$$

3. Express $|\tau_{\alpha_1 i_2}^{[3\ldots n]}\rangle$ by at most χ Schmidt vectors $|\Phi_{\alpha_2}^{[3\ldots n]}\rangle$(the eigenvectors of $\rho^{[3\cdots n]}$), where α_2 ranges from 1 to χ and $\chi = \max_A \chi_A$, here χ_A denotes the rank of the reduced density matrix ρ_A for a particular partition $A : B$ of the n-qubit state:

$$|\tau_{\alpha_1 i_2}^{[3\ldots n]}\rangle = \sum_{\alpha_2} \Gamma_{\alpha_1\alpha_2}^{[2]i_2} \lambda_{\alpha_2}^{[2]} |\Phi_{\alpha_2}^{[3\ldots n]}\rangle, \tag{357}$$

   where $\lambda_{\alpha_2}^{[2]}$'s are the corresponding Schmidt coefficients.

4. Subsitute (356) and (357) into (354), we get

$$|\Psi\rangle = \sum_{i_1,\alpha_1,i_2,\alpha_2} \Gamma_{\alpha_1}^{[1]i_1} \lambda_{\alpha_1}^{[1]} \Gamma_{\alpha_1\alpha_2}^{[2]i_2} \lambda_{\alpha_2}^{[2]} |i_1 i_2\rangle |\Phi_{\alpha_2}^{[3\ldots n]}\rangle. \tag{358}$$

   Now it's easy to see if we repeat the steps 2-4, we get the expansion of $|\Psi\rangle$ in the computational basis:

$$|\Psi\rangle = \sum_{i_1} \ldots \sum_{i_n} c_{i_1\ldots i_n} |i_1\rangle \ldots |i_n\rangle, \tag{359}$$

   where the coefficients $c_{i_1\ldots i_n}$ are

$$c_{i_1\ldots i_n} = \sum_{\alpha_1,\ldots,\alpha_{n-1}} \Gamma_{\alpha_1}^{[1]i_1} \lambda_{\alpha_1}^{[1]} \Gamma_{\alpha_1\alpha_2}^{[2]i_2} \lambda_{\alpha_2}^{[2]} \ldots \Gamma_{\alpha_{n-1}}^{[n]i_n}. \tag{360}$$

Through comparing equations (348) and (360), we are able to construct $V_0^{[k]i_k}$ and $V_1^{[k]i_k}$ explicitly. The detailed work is omitted here since in next section about the more general $N \to M$ sequential cloning case, each step of getting the matrix is provided.

When the input state of the cloning machine is an arbitrary state $|\psi\rangle = x_0|0\rangle + x_1|1\rangle$(normalization condition is satisfied: $|x_0|^2 + |x_1|^2 = 1$.), according to the linearity principle of quantum mechanics, the state after cloning transformation is $x_0|\Psi_M^{(0)}\rangle + x_1|\Psi_M^{(1)}\rangle$, which can also be sequentially generated. First, view the arbitrary state $|\psi\rangle$ and the ancilla's initial state $|0\rangle_D$ as a unified state: $|\phi_I\rangle = |\psi\rangle \otimes |0\rangle_D$. Then use the qubit k,$(k = 1, 2, ..., n)$, sequentially

to interact with the ancilla according to the 2D-dimensional isometric operators $V^{[k]i_k} = |0\rangle\langle 0|\otimes V_0^{[k]i_k} + |1\rangle\langle 1|\otimes V_1^{[k]i_k}$. After all qubits have interacted with the ancilla, perform a generalized Hadamard transformation to the ancilla

$$|0\rangle|\phi_F^{(0)}\rangle \to \frac{1}{\sqrt{2}}[|0\rangle|\phi_F^{(0)}\rangle + |1\rangle|\phi_F^{(1)}\rangle] \tag{361}$$

$$|1\rangle|\phi_F^{(1)}\rangle \to \frac{1}{\sqrt{2}}[|0\rangle|\phi_F^{(0)}\rangle - |1\rangle|\phi_F^{(1)}\rangle] \tag{362}$$

Now measure the ancilla with the basis $\{|0\rangle|\phi_F^{(0)}\rangle, |1\rangle|\phi_F^{(1)}\rangle\}$, either result occurs with probability 1/2. When the result is $|0\rangle|\phi_F^{(0)}\rangle$, we get the desired state $x_0|\Psi_M^{(0)}\rangle + x_1|\Psi_M^{(1)}\rangle$; while if the result is $|1\rangle|\phi_F^{(1)}\rangle$, we need to perform a π-phase gate upon each qubit, and the desired state will be obtained.

To realized the above $1 \to M$ cloning scheme, an ancilla system of dimension $2M$ is needed, while if we take a global unitary operation to accomplish the cloning, the dimension of the unitary operation will increase exponentially with M. So we see sequential cloning is much easier to realize experimentally.

B. $N \to M$ optimal sequential UQCM

In this section, we will discuss the more general case $N \to M$ optimal sequential UQCM. An arbitrary qubit is written $|\Psi\rangle = x_0|0\rangle + x_1|1\rangle(|x_0|^2 + |y_0|^2 = 1)$, then N identical $|\Psi\rangle$ can be expressed as

$$|\Psi\rangle^{\otimes N} = \sum_{m=0}^{N} x_0^{N-m} x_1^m \sqrt{C_N^m}|(N-m)0, m1\rangle, \tag{363}$$

where $C_N^m = \frac{N!}{m!(N-m)!}$, and $|(N-m)0, m1\rangle$ denotes the normalized completely symmetric N-qubit state with (N-m) qubits in state $|0\rangle$ and m qubits in state $|1\rangle$.

It is well known that the optimal UQCM transformation for completely symmetric states(Gisin and Massar, 1997) is

$$|(N-m)0, m1\rangle \otimes |R\rangle \to |\Psi_M^{(m)}\rangle = \sum_{j=0}^{M-N} \beta_{mj}|(M-m-j)0, (m+j)1\rangle \otimes |R_j\rangle, \tag{364}$$

where $\beta_{mj} = \sqrt{C_{M-m-j}^{M-N-j} C_{m+j}^{j} / C_{M+1}^{N+1}}$, R_j denotes the final states of the cloning machine, and for different j, $|R_j\rangle$'s are orthogonal to each other. Here we can choose $|R_j\rangle = |(M-N-j)1, j0\rangle_R$. Since we have found the cloning transformation of any state in the form $|((N-m)0, m1\rangle$, according to the linearity principle of quantum mechanics, the transformation for N arbitrary state $|\Psi\rangle$ is

$$|\Psi\rangle^{\otimes N} \otimes |R\rangle \to |\Psi_M\rangle = \sum_{m=0}^{N} x_0^{N-m} x_1^m \sqrt{C_N^m}|\Psi_M^{(m)}\rangle, \tag{365}$$

here $|\Psi_M\rangle$ is the final state of all the qubits and the cloning machine we hope to obtain, like the $1 \to N$ sequential UQCM case, we first need to show how $|\Psi_M^{(m)}\rangle$ can be sequentially generated. Hence it's necessary to know the MPS form of $|\Psi_M^{(m)}\rangle$:

$$|\Psi_M^{(m)}\rangle = \sum_{i_1 \ldots i_{2M-N}} \langle\phi_F|V^{[2M-N]i_{2M-N}} \ldots V^{[1]i_1}|\phi_I\rangle|i_1 \ldots i_{2M-N}\rangle, \tag{366}$$

where $V^{[n]i_n}(1 \le n \le 2M-N)$ is a $D \times D$ dimensional matrix, and satisfies the isometry condition:$\sum_{i_n}(V^{[n]i_n})^\dagger V^{[n]i_n} = I$. Now we shall follow the idea of SD, and give detailed elaboration on how to get the explicit form of $V^{[n]i_n}$.

1. Case $n = 1$.

Compute the SD of $|\Psi_M^{(m)}\rangle$ according to partition 1:2...(2M-N):

$$\begin{aligned}\left|\Psi_M^{(m)}\right\rangle &= \sum_{j=0}^{M-N}\beta_{mj}\,|(M-m-j)\,0,(m+j)\,1\rangle\otimes|R_j\rangle \\ &= \sum_{\alpha_1}\lambda_{\alpha_1}^{[1]}|\phi_{\alpha_1}^{[1]}\rangle\otimes|\phi_{\alpha_1}^{[2\ldots(2M-N)]}\rangle \\ &= \sum_{\alpha_1,i_1}\Gamma_{\alpha 1}^{[1]i_1}\lambda_{\alpha_1}^{[1]}|i_1\rangle\otimes|\phi_{\alpha_1}^{[2\ldots(2M-N)]}\rangle \\ &= |0\rangle\otimes\lambda_1^{[1]}\left|\phi_1^{[2\ldots(2M-N)]}\right\rangle+|1\rangle\otimes\lambda_2^{[1]}\left|\phi_2^{[2\ldots(2M-N)]}\right\rangle,\end{aligned} \tag{367}$$

where through comparing the first and last lines, we get

$$\left|\phi_1^{[2\ldots(2M-N)]}\right\rangle=\sum_{k=-m}^{M-m-1}\beta_{mk}\sqrt{\frac{C_{M-1}^{m+k}}{C_M^{m+k}}}\,|(M-m-k-1)\,0,(m+k)\,1\rangle\otimes|R_k\rangle/\lambda_1^{[1]},$$

$$\left|\phi_2^{[2\ldots(2M-N)]}\right\rangle=\sum_{k=-m}^{M-m-1}\beta_{m(k+1)}\sqrt{\frac{C_{M-1}^{m+k}}{C_M^{m+k+1}}}\,|(M-m-k-1)\,0,(m+k)\,1\rangle\otimes|R_{k+1}\rangle/\lambda_2^{[1]}.$$

Compare the last two lines, we also have

$$\Gamma_{\alpha_1}^{[1]0}=\delta_{\alpha_1,1},\ \Gamma_{\alpha_1}^{[1]1}=\delta_{\alpha_1,2},\ \alpha_1=1,2.$$

Now use the condition of normalization, Schmidt coefficients could be calculated,

$$\lambda_1^{[1]}=\sqrt{\sum_{k=-m}^{M-m-1}\beta_{mk}^2\frac{C_{M-1}^{m+k}}{C_M^{m+k}}},\ \lambda_2^{[1]}=\sqrt{\sum_{k=-m}^{M-m-1}\beta_{m(k+1)}^2\frac{C_{M-1}^{m+k}}{C_M^{m+k+1}}}.$$

Then we have

$$V_{\alpha_1}^{[1]i_1}=\Gamma_{\alpha_1}^{[1]i_1}\lambda_{\alpha_1}^{[1]}.$$

The explicit form of $V^{[1]i_1}$ is given in the appendix, so is other $V^{[i]i_n}$.

Next, we will not present the detailed calculations for other cases since the method is almost the same, but only list the results.

2. For $1<n\le M-1$: We calculate the SD of $|\Psi_M^{(m)}\rangle$ according to partitions. The results are:

$$\lambda_{j+1}^{[n]}=\sqrt{C_n^j\sum_{k=-m}^{M-m-n}\beta_{m(j+k)}^2\frac{C_{M-n}^{m+k}}{C_M^{m+j+k}}},\quad \lambda_{j+1}^{[n-1]}=\sqrt{C_{n-1}^j\sum_{k=-m}^{M-m-n+1}\beta_{m(j+k)}^2\frac{C_{M-n+1}^{m+k}}{C_M^{m+j+k}}}.$$

$$\Gamma_{(j+1)\alpha_n}^{[n]0}=\delta_{(j+1)\alpha_n}\frac{\sqrt{C_{n-1}^j}}{\lambda_{j+1}^{[n-1]}\sqrt{C_n^j}},\quad \Gamma_{(j+1)\alpha_n}^{[n]1}=\delta_{(j+2)\alpha_n}\frac{\sqrt{C_{n-1}^j}}{\lambda_{j+1}^{[n-1]}\sqrt{C_n^{j+1}}}.$$

And for this case, the summarized form is $V_{\alpha_n\alpha_{n-1}}^{[n]i_n}=\Gamma_{\alpha_{n-1}\alpha_n}^{[n]i_n}\lambda_{\alpha_n}^{[n]}$.

3. Case $n=M$: We have,

$$\lambda_{j+1}^{[M]}=\beta_{m(j-m)},\quad \lambda_{j+1}^{[M-1]}=\sqrt{C_{M-1}^j\sum_{k=-m}^{-m+1}\beta_{m(j+k)}^2\frac{C_1^{m+k}}{C_M^{m+j+k}}}.$$

And also,

$$\Gamma^{[M]0}_{(j+1)\alpha_M} = \delta_{\alpha_M(j+1)} \frac{\sqrt{C^j_{M-1}}}{\lambda^{[M-1]}_{j+1}\sqrt{C^j_M}},$$

$$\Gamma^{[M]1}_{(j+1)\alpha_M} = \delta_{\alpha_M(j+2)} \frac{\sqrt{C^j_{M-1}}}{\lambda^{[M-1]}_{j+1}\sqrt{C^{j+1}_M}}.$$

Similarly, for this case $V^{[M]i_M}_{\alpha_M\alpha_{M-1}} = \Gamma^{[M]i_M}_{\alpha_{M-1}\alpha_M}\lambda^{[M]}_{\alpha_M}$.

4. Case $M+l$ $(1 \le l \le M-N)$: We have,

$$\lambda^{[M+l]}_{j+1} = \sqrt{C^{j-m}_{M-N-l}\sum_{k=0}^{l}\beta^2_{m(j+k-m)}\frac{C^k_l}{C^{j+k-m}_{M-N}}}.$$

$$\lambda^{[M+l-1]}_{j+1} = \sqrt{C^{j-m}_{M-N-l+1}\sum_{k=0}^{l-1}\beta^2_{m(j+k-m)}\frac{C^k_{l-1}}{C^{j+k-m}_{M-N}}},$$

$$\Gamma^{[M+l]0}_{(j+1)\alpha_{M+l}} = \delta_{\alpha_{M+l}j}\sqrt{\frac{C^{j-m-1}_{M-N-l}}{C^{j-m}_{M-N-l+1}}}/\lambda^{[M+l]}_{\alpha_{M+l}},$$

$$\Gamma^{[M+l]1}_{(j+1)\alpha_{M+l}} = \delta_{\alpha_{M+l}(j+1)}\sqrt{\frac{C^{j-m}_{M-N-l}}{C^{j-m}_{M-N-l+1}}}/\lambda^{[M+l]}_{\alpha_{M+l}}.$$

Then we have $V^{[M+l]i_{M+l}}_{\alpha_{M+l}\alpha_{M+l-1}} = \Gamma^{[M+l]i_{M+l}}_{\alpha_{M+l-1}\alpha_{M+l}}\lambda^{[M+l]}_{\alpha_{M+l}}$.

Up till now, we have calculated out the explicit form of every $V^{[k]i_k}$, and since $V^{[k]i_k}$ depends on m, we denote it as $V^{[k]i_k}_{(m)}$ here after. Through computation, we can get the smallest dimension needed for the isometric operator $V_(m)^{[k]i_k}$,

$$D = \{ \begin{array}{ll} M - N/2 + 1 & \text{if N is even;} \\ M - (N-1)/2 + 1 & \text{if N is odd.} \end{array} \tag{368}$$

So we see D increases linearly with M, which shall significantly ease the difficulty of sequential cloning.

Based on the above computation, we have known that the state $|\Psi^{(m)}_M\rangle$ can be expressed in the MPS form, so the N-qubit pure state $|(N-m)0, m1\rangle$ can be sequentially transformed to $|\Psi^{(m)}_M\rangle$. Now in order to sequentially clone the N-qubit $|\Psi\rangle^{\otimes N}$ to M qubits, the scheme is as follows(Dang and Fan, 2008).

1). Encode the N-qubit $|\Psi\rangle^{\otimes N}$ in the ancilla, which makes the initial state of the united ancilla

$$|\phi^{'}_I\rangle = \sum_{m=0}^{N} x_0^{N-m}x_1^m\sqrt{C^m_N}|(N-m)0, m1\rangle \otimes |0\rangle_D. \tag{369}$$

2). Build the operators

$$V^{[k]i_k} = \sum_{m=0}^{N}(\sqrt{C^m_N})^{\frac{1}{2M-N}}(|0\rangle\langle 0|)^{\otimes N-m}(|1\rangle\langle 1|)^{\otimes m} \otimes V^{[n]i_n}_{(m)}. \tag{370}$$

3). Let all the qubits interact sequentially with the united ancilla according to the operator $V^{[k]i_k}$, we get the final state of the whole system

$$|\Psi_{out}\rangle = \sum_{i_1...i_{2M-N}} V^{[2M-N]i_{2M-N}}...V^{[1]i_1}|\varphi_i^{'}\rangle \otimes |i_1...i_{2M-N}\rangle$$
$$= \sum_{m=0}^{N} x_0^{N-m} x_1^m \sqrt{C_N^m}|0\rangle^{\otimes N-m}|1\rangle^{\otimes m} \otimes |\varphi_F^{(m)}\rangle \otimes |\Psi_M^{(m)}\rangle,$$

where $|\varphi_F^{(m)}\rangle$ is the final state of the ancilla when the input state is $|(N-m)0, m1\rangle$.

4). Perform a generalized Hadamard gate on the ancilla (quantum fourier transformation)

$$|0\rangle^{\otimes N-m}|1\rangle^{\otimes m} \otimes |\varphi_F^{(m)}\rangle \to \frac{1}{\sqrt{N+1}} \sum_{m'=0}^{N} e^{\frac{i2\pi mm'}{N+1}} |0\rangle^{\otimes N-m'}|1\rangle^{\otimes m'} \otimes |\varphi_F^{(m')}\rangle, \tag{371}$$

after which the final state becomes

$$|\Psi_{out}^{'}\rangle = \frac{1}{\sqrt{N+1}} \sum_{m'=0}^{N} |0\rangle^{\otimes N-m'}|1\rangle^{\otimes m'} \otimes |\varphi_F^{(m')}\rangle \otimes |\Psi_M^{'}\rangle, \tag{372}$$

where

$$|\Psi_M^{'}\rangle = \sum_{m=0}^{N} e^{\frac{i2\pi mm'}{N+1}} x_0^{N-m} x_1^m \sqrt{C_N^m}|\Psi_M^{(m)}\rangle. \tag{373}$$

5). Make measurement on the whole ancilla with the basis $\{|0\rangle^{\otimes N-m'}|1\rangle^{\otimes m'} \otimes |\varphi_F^{(m')}\rangle\}_{m'=0}^{N}$. When the result is $m'=0$, the desired state $|\Psi_M\rangle = \sum_{m=0}^{N} x_0^{N-m} x_1^m \sqrt{C_N^m}|\Psi_M^{(m)}\rangle$ is directly obtained. If the measured $m' \neq 0$, then we need to act a local phase gate U_S on every qubit. Through computation, a proper phase gate is

$$U_S = |0\rangle\langle 0| + e^{i\theta}|1\rangle\langle 1|, \tag{374}$$

where $\theta = -\frac{2\pi m'}{N+1}$. With the effect of the phase gate, the output state becomes

$$|\Psi_M^{''}\rangle = e^{i(M-N)\theta}|\Psi_M\rangle. \tag{375}$$

Since the phase $e^{i(M-N)\theta}$ won't affect, the output state is what we want. Now it can be seen we have realized the sequential $N \to M$ UQCM. When $N=1$, all the results coincide with the $1 \to M$ case in last section.

Recently, the sequential cloning concerning about the real-life experimental condition is investigated in (Saberi and Mardoukhi, 2012).

C. Sequential UQCM in d dimensions

We now further proceed to a more general case where qubit is extended to qudit. In the space of d dimensions, an arbitrary quantum pure state can be expressed as

$$|\Psi\rangle = \sum_{i=0}^{d-1} x_i|i\rangle, \sum_{i=0}^{d-1} |x_i|^2 = 1. \tag{376}$$

Then N identical such qudits will be expanded in symmetric space as(Werner, 1998)

$$|\Psi\rangle^{\otimes N} = \sum_{\boldsymbol{m}=0}^{N} \sqrt{\frac{N!}{m_1!...m_d!}} x_0^{m_1}...x_{d-1}^{m_d}|\boldsymbol{m}\rangle, \tag{377}$$

where $|\boldsymbol{m}\rangle$ denotes the symmetric state, whose form is

$$|\boldsymbol{m}\rangle = |m_1 0, m_2 1, ..., m_d(d-1)\rangle, \tag{378}$$

which means the symmetric state $|\boldsymbol{m}\rangle$ has m_i qudits in the computational base $|i\rangle$(i=1,...,d), and the sum of qubits in each base satisfies $\sum_{i=1}^{d} m_i = N$.

Take the symmetric state $|\boldsymbol{m}\rangle$ as the input state of the optimal d-level UQCM according to Fan et al's scheme(Fan *et al.*, 2001a), the corresponding M-qudit output state will be

$$|\Psi_M^{(\boldsymbol{m})}\rangle = \sum_{\boldsymbol{j}=0}^{M-N} \beta_{\boldsymbol{m}\boldsymbol{j}} |\boldsymbol{m}+\boldsymbol{j}\rangle \otimes |R_{\boldsymbol{j}}\rangle, \tag{379}$$

where the vector $\boldsymbol{j} = (j_1, j_2, ...j_d)$ satisfies $\sum_{i=1}^{d} j_i = M - N$, $|R_{\boldsymbol{j}}\rangle = |\boldsymbol{j}\rangle_R$ denotes the state of the cloning machine, and $\beta_{\boldsymbol{m}\boldsymbol{j}} = \sqrt{\prod_{i=1}^{d} C_{m_i+j_i}^{m_i} / C_{M+d-1}^{M-N}}$. The following steps are similar to the 2-level case presented previously. We still need to find the MPS form of the state $|\Psi_M^{(\boldsymbol{m})}\rangle$, and the method is through SD as well. Express $|\Psi_M^{(\boldsymbol{m})}\rangle$ in the computational basis

$$|\Psi_M^{(\boldsymbol{m})}\rangle = \sum_{i_1...i_{2M-N}} \langle \varphi_F^{(\boldsymbol{m})}| V^{[2M-N]i_{2M-N}} ... V^{[1]i_1} |0\rangle_D \otimes |i_1...i_{2M-N}\rangle \tag{380}$$

Through computation, $V^{[k]i_k}$ can be obtained(Dang and Fan, 2008), whose detailed process is just a direct extension of the 2-level case and shall be omitted here, the result is provided in the Appendix. Besides, we will also know that the necessary dimension of the ancilla is $D_d = C_{M-\lfloor\frac{N+1}{2}\rfloor+d-1}^{M-\lfloor\frac{N+1}{2}\rfloor}$, where the symbol $\lfloor X \rfloor$ denotes the floor function. So we see when $d \geq 2$ D_d is far smaller than d_M, which shows the advantage of sequential cloning of qudits.

XI. IMPLEMENTATION OF QUANTUM CLONING MACHINES IN PHYSICAL SYSTEMS

In general, the cloning machines can be realized by the corresponding quantum circuits constituted by single qubit rotation gates and CNOT gates just like other quantum computations. This is guaranteed by the universal quantum computation (Barenco *et al.*, 1995).

A. A unified quantum cloning circuit

It is interesting that the UQCM and the phase-covariant QCM can be realized by a unified quantum cloning circuit by adjusting angles in the single qubit rotation gates, as shown in FIG.11 first presented by Bužek *et al.* (Bužek *et al.*, 1997a). Let us consider the definition of single qubit rotation gate (33) with a fixed phase parameter which can be omitted, it can be written in matrix form as,

$$\hat{R}(\vartheta) = \begin{pmatrix} \cos\vartheta & \sin\vartheta \\ -\sin\vartheta & \cos\vartheta \end{pmatrix}. \tag{381}$$

The form of CNOT gate is in (34). Here we use subindices in a CNOT gate, $CNOT_{jk}$, to specify that the controlled qubit is j and the target qubit is k. Following the copying scheme in (Bužek *et al.*, 1997a), the cloning procession is divided into two unitary transformations,

$$|\Psi^{(in)}_{a_1}|0\rangle_{a_2}|0\rangle_{a_3} \rightarrow |\Psi\rangle^{(in)}_{a_1}|\Psi\rangle^{(prep)}_{a_1a_2} \rightarrow |\Psi\rangle^{(out)}_{a_1a_2a_3}. \tag{382}$$

The preparation state is constructed as follows,

$$|\Psi\rangle^{(prep)}_{a_2a_3} = \hat{R}_2(\vartheta_3)CNOT_{32}\hat{R}_3(\vartheta_2)CNOT_{23}\hat{R}_2(\vartheta_1)|0\rangle_{a_2}|0\rangle_{a_3}. \tag{383}$$

The second step is as,

$$|\Psi\rangle^{(out)}_{a_1a_2a_2} = CNOT_{a_3a_1}CNOT_{a_2a_1}CNOT_{a_1a_3}CNOT_{a_1a_2}|\psi\rangle^{(in)}_{a_1}|\psi\rangle^{(prep)}_{a_2a_3}. \tag{384}$$

We may find that two copies are in a_2, a_3 qubits. For UQCM, the angles in the single qubit rotations are chosen as,

$$\vartheta_1 = \vartheta_3 = \frac{\pi}{8}, \quad \vartheta_2 = -\arcsin\left(\frac{1}{2} - \frac{\sqrt{2}}{3}\right)^{1/2}. \tag{385}$$

This scheme is flexible and can be adjusted for phase-covariant quantum cloning. We only need to choose different angles for the single qubit rotations, and those angles are shown to be as follows (Fan *et al.*, 2001b),

$$\vartheta_1 = \vartheta_3 = \arcsin\left(\frac{1}{2} - \frac{1}{2\sqrt{3}}\right)^{\frac{1}{2}}, \quad \vartheta_2 = -\arcsin\left(\frac{1}{2} - \frac{\sqrt{3}}{4}\right)^{\frac{1}{2}}. \tag{386}$$

To be explicit, we may find that the preparation state takes the form,

$$|\Psi\rangle^{(perp)}_{a_2a_3} = \frac{1}{\sqrt{2}}|00\rangle_{a_2a_3} + \frac{1}{2}(|01\rangle_{a_2a_3} + |10\rangle_{a_2a_3}). \tag{387}$$

The second step for phase-covariant quantum cloning is the same as the that of the UQCM. So this cloning circuit is general and can be applied for both universal cloning and phase-covariant cloning.

B. A simple scheme of realization of UQCM and Valence-Bond Solid state

We already know that the universal cloning machine can be realized by a symmetric projection. This fact can let us find a simple scheme for the implementation of the universal cloning machine. The simplest universal cloning machine can be obtained by a symmetric projection on the input qubit and one part of a maximally entangled state. This symmetric projection can be naturally realized by bosonic operators in the Fock space representation. Suppose the input state is $a^\dagger_H$, the available maximally entangled state is $a^\dagger_H a^\dagger_H + a^\dagger_V a^\dagger_V$, here H, V can be horizontal and

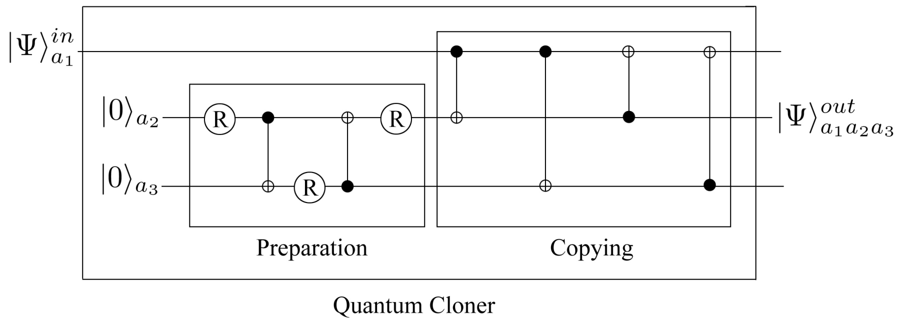


FIG. 11 Quantum circuit implementing quantum cloning machines. This quantum circuit can realize both universal cloning machine and phase-covariant quantum cloning machine by adjusting parameters in the single qubit rotation gates. This circuit is the same as the one in (Bužek *et al.*, 1997a).

vertical polarizations of a photon, or any other degrees of freedom of the bosonic operator. We also suppose that those operators are acting on the vacuum state, then we have,

$$a_H^\dagger\left(a_H^\dagger a_H^\dagger + a_V^\dagger a_V^\dagger\right) = \left[\sqrt{\frac{2}{3}}\frac{(a_H^\dagger)^2}{\sqrt{2!}}a_H^\dagger + \sqrt{\frac{1}{3}}(a_H^\dagger a_V^\dagger)a_V^\dagger\right]\sqrt{3}. \tag{388}$$

Now we consider that the last bosonic operators are acting as ancillary qubits, in Fock space representation, $\frac{(a_H^\dagger)^2}{\sqrt{2}}$ corresponds to two photons in horizontal polarization, while $a_H^\dagger a_V^\dagger$ is a symmetric state with one horizontal photon and one vertical photon. By a whole normalization factor $\sqrt{3}$, the above formula then takes the following form, with initial state $|H\rangle$,

$$|H\rangle \to \sqrt{\frac{2}{3}}|2H\rangle|H\rangle_a + \sqrt{\frac{1}{3}}|H,V\rangle\rangle|V\rangle_a. \tag{389}$$

Similarly for a vertical photon, we have

$$|V\rangle \to \sqrt{\frac{2}{3}}|2V\rangle|V\rangle_a + \sqrt{\frac{1}{3}}|H,V\rangle\rangle|H\rangle_a. \tag{390}$$

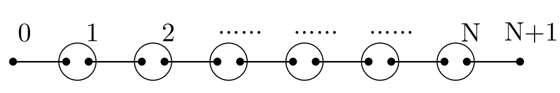
It is now clear that those two transformations constitute exactly a UQCM. This fact is noticed by Simon *et al.*. Actually it also provides a natural realization of the UQCM by photon stimulated emission. Based on the experiment of the preparation of maximally entangled state, the UQCM can be realized by the above scheme which we will present later.

For no-cloning theorem, a frequently misunderstanding point may be that, it seems that “laser” itself can provide a perfect cloning machine, one photon can be cloned perfectly to have many completely same photons. This seems contradict with no-cloning theorem. The point is that we can for sure clone a photon to have may copies. However, the no-cloning theorem states that if we clone horizontal and vertical photons perfectly, we can not clone perfectly the photon superposition state of horizontal and vertical. Thus “laser” does not conflict with no-cloning theorem.

When a maximally entangled state is available, it seems that a UQCM can be realized. In condensed matter physics, the Valence-Bond Solid state is constructed by a series of singlet states, see for example (Fan *et al.*, 2004),

$$|VBS\rangle = \prod_{i=0}^{N}\left(a_i^\dagger b_{i+1}^\dagger - a_{i+1}^\dagger b_i^\dagger\right)|\text{vacuum}\rangle, \tag{391}$$

where sites 0 and $N+1$ are two ends. We remark that the sites in the bulk will be restricted to the symmetric subspace also by the reason of Fock space representation as shown schematically in the following:



By the same consideration as presented above, since one singlet state is a maximally entangled state, the UQCM can be realized if the input state is put in site 0, $(\alpha a_0^\dagger + \beta b_0^\dagger)\left(a_0^\dagger b_1^\dagger - a_1^\dagger b_0^\dagger\right)$. Further one may notice we do not need to restrict just a singlet state where only two sites are involved, a whole one-dimensional Valence-Bond Solid state can be dealed as a maximally entangled state so that a UQCM can be realized like the following:

$$(\alpha a_0^\dagger + \beta b_0^\dagger)|VBS\rangle. \tag{392}$$

The state of input $\alpha a_0^\dagger + \beta b_0^\dagger$ is like the open boundary operator. One feature of this universal cloning machine may be that the ancillary states are at one end of this 1D state, the two copies are located on another end. This system is like a majorana fermion quantum wire proposed by Kitaev (Kitaev, 2001) where the encoded qubit is topologically protected. It is also pointed out that the cloning machine can be realized by networks of spin chains (De Chiara *et al.*, 2004).

C. UQCM realized by photon stimulated emission

With the results in last section, one may realize that a maximally entanglement source may provide a mechanism for quantum cloning. The corresponding fidelity is optimal. It seems that photon stimulated emission possesses such a property and can give a realization of the UQCM. This is first proposed in (Kempe *et al.*, 2000; Simon *et al.*, 2000) and realized experimentally (Fasel *et al.*, 2002; Lamas-Linares *et al.*, 2002). In this scheme, certain types of three-level atoms can be used to optimality clone qubit that is encoded as an arbitrary superposition of excitations in the photonic modes corresponding to the atomic transitions. Next, we shall first review briefly the qubit case followed by a general d-dimensional result.

For qubit case (Kempe *et al.*, 2000; Simon *et al.*, 2000), we consider the inverted medium that consists of an ensemble of Λ atoms with three energy levels. These three levels correspond to two degenerate ground states $|g_1\rangle$ and $|g_2\rangle$ and an excited level $|e\rangle$. The ground states are coupled to the excited state by two modes of the electromagnetic field a_1 and a_2, respectively. The Hamiltonian of this system takes the form,

$$H = \gamma\left(a_1\sum_{k=1}^{N}|e^k\rangle\langle g_1^k| + a_2\sum_{k=1}^{N}|e^k\rangle\langle g_2^k|\right) + H.c. \tag{393}$$

We then introduce the operator as $b_r c^\dagger \equiv \sum_{k=1}^{N}|e^k\rangle\langle g_r^k|, \quad r = 1,2$, where $c^\dagger$ is a creation operator of "e-type" excitation, b_r is a annihilation operator of g_r ground states, $r = 1,2$. Now the Hamiltonian (393) becomes as,

$$\mathcal{H} = \gamma(a_1 b_1 + a_2 b_2)c^\dagger + H.c. \tag{394}$$

Now we find that the source of maximally entangled states is available. The input state can be considered as the form $(\alpha a_1^\dagger + \beta a_2^\dagger)|0,0\rangle = \alpha|1,0\rangle + \beta|0,1\rangle$. The number of copies in this cloning system is restricted by the number of atoms in excited states $\otimes_{k=1}^{N}|e^k\rangle$ which are represented as $(c^\dagger)^N/\sqrt{N!}$. We may consider that initially there are $i+j$ qubits in $a_1^\dagger$ and $a_2^\dagger$ which corresponds to a completely symmetric state with i,j states in two different levels of qubits,

$$\begin{aligned}|\Psi_{in},(i,j)\rangle &= \frac{(a_1^\dagger)^i(a_2^\dagger)^j(c^\dagger)^N}{\sqrt{i!j!N!}}|0\rangle \\ &= |i_{a_1}, j_{a_2}\rangle|0_{b_1}, 0_{b_2}\rangle|N_c\rangle \\ &\equiv |i,j\rangle_a|0,0\rangle_b|N\rangle_c.\end{aligned} \tag{395}$$

With the Hamiltonian (394), the time evolution of the state starting from the initial state (395) becomes as follows,

$$\begin{aligned}&|\Psi(t),(i,j)\rangle = e^{-iHt}|\Psi_{in},(i,j)\rangle \\ &= \sum_p(-iHt)^p/p!|\Psi_{in},(i,j)\rangle = \sum_{l=0}^{N} f_l(t)|F_l,(i,j)\rangle,\end{aligned} \tag{396}$$

where $|\Psi_{in},(i,j)\rangle = |F_0,(i,j)\rangle$, l is the additional photons emitted corresponding to additional copies, thus there are altogether $i+j+l$ copies in the output which is expressed as $|F_l,(i,j)\rangle$. In this process, the states with different copies are actually superposed together. The amplitude parameter in the superposed state corresponds to the probability of finding l additional copies which is $|f_l(t)|^2$.

To show that this process is exactly the realization of the optimal UQCM, we can show that the corresponding cloning transformation with l additional copes can be calculated as,

$$|i,j\rangle_a|0,0\rangle_b|N\rangle_c \to |F_l,(i,j)\rangle = \sum_{k=0}^{l}\sqrt{\frac{l!(i+j+1)!}{(i+j+l+1)!}}\sqrt{\frac{(i+l-k)!(j+k)!}{i!j!k!(l-k)!}} \\ |i+l-k,j+k\rangle_a|l-k,k\rangle_b|N-l\rangle_c. \tag{397}$$

This is indeed the UQCM. In addition, this provides an alternative method to find the optimal cloning transformations.

The higher dimensional case can be similarly studied (Fan *et al.*, 2002). Now the atoms have one excited state $|e\rangle$ and d ($d \geq 2$) ground states $|g_n\rangle, n = 1, 2, \cdots, d$, and each coupled to a different photons a_n corresponding to modes of qudit. The Hamiltonian can also be written as a generalized form,

$$\mathcal{H}_d = \gamma(a_1 b_1 + \cdots + a_d b_d) + H.c. \tag{398}$$

The initial states which are symmetric states are,

$$|\Psi_{in}, \vec{j}\rangle = \prod_{i=1}^{d}\frac{(a_i^\dagger)^{j_i}}{\sqrt{j_i!}}\frac{(c^\dagger)^N}{\sqrt{N!}}|0\rangle \equiv |\vec{j}\rangle_a|\vec{0}\rangle_b|N\rangle_c, \tag{399}$$

where $\vec{j} = (j_1, j_2, \cdots, j_d)$. One can find that the time evolution of states for qudits is the same as that of qubits (396). So the probability to obtain additional l copies is $|f_l(t)|^2$. We use the notation $|F_0, \vec{j}\rangle \equiv |\Psi_{in}, \vec{j}\rangle$, $\sum_i j_i = M$, and the output of cloning with l additional copies can be obtained as,

$$\begin{aligned} |\vec{j}\rangle_a|\vec{0}\rangle_b|N\rangle_c \to |F_l, \vec{j}\rangle &= \sum_{k_i}^{l}\sqrt{\frac{(M+d-1)!l!}{(M+l+d-1)!}}\prod_{i=1}^{d}\sqrt{\frac{(k_i+j_i)!}{k_i!j_i!}} \\ &\quad |\vec{j}+\vec{k}\rangle_a|\vec{k}\rangle_b|N-l\rangle_c, \end{aligned} \tag{400}$$

where summation $\sum_{k_i}^{l}$ runs for all variables with constraint, $\sum_i^d k_i = l$. We thus realize the optimal UQCM for qudits.

Explicitly, the action of Hamiltonian on the symmetric states takes the following form,

$$\begin{aligned} &\mathcal{H}_d|F_l, \vec{j}\rangle = \gamma(\sqrt{(l+1)(N-l)(M+l+d)}|F_{l+1}, \vec{j}\rangle \\ &+\sqrt{l(N-l+1)(M+l+d-1)}|F_{l-1}, \vec{j}\rangle, \\ &\quad l \leq l < N, \\ &\mathcal{H}_d|F_0, \vec{j}\rangle = \gamma\sqrt{N(M+d)}|F_1, \vec{j}\rangle, \\ &\mathcal{H}_d|F_N, \vec{j}\rangle = \gamma\sqrt{N(M+N+d-1)}|F_{N-1}, \vec{j}\rangle. \end{aligned} \tag{401}$$

To end this subsection, we present our familiar results of UQCM but in this photonic system. An arbitrary qudit takes the form, $|\Psi\rangle = \sum_{i=1}^d x_i a_i^\dagger|\vec{0}\rangle$, with $\sum_{i=1}^d |x_i|^2 = 1$. By expansion, it corresponds to state,

$$\begin{aligned} |\Psi\rangle^{\otimes M} &= (\sum_{i=1}^{d} x_i a_i^\dagger)^{\otimes M}|\vec{0}\rangle \\ &= M!\sum_{j_i}^{M}\prod_{i=1}^{d}\frac{x_i^{j_i}}{\sqrt{j_i!}}\frac{(a_i^\dagger)^{j_i}}{\sqrt{j_i!}}|\vec{0}\rangle. \end{aligned} \tag{402}$$

With the help of cloning transformation (400), the output of cloning is,

$$\begin{aligned} |\Psi\rangle^{\otimes M} \to |\Psi\rangle^{out} &= M!\sum_{j_i}^{M}\sum_{k_i}^{l}\sqrt{\frac{(M+d-1)!l!}{(L+d-1)!}} \\ &\quad \times \prod_{i=1}^{d}\frac{x_i^{j_i}}{j_i!}\sqrt{\frac{(k_i+j_i)!}{k_i!}}|\vec{j}+\vec{k}\rangle_a|\vec{k}\rangle_b, \end{aligned} \tag{403}$$

As we already know, this is the UQCM of qudits.

Quantum cloning itself is reversible since it is realized by unitary transformation. This does not necessarily mean that the cloning realized by photon stimulated emission can be inverted. However, it is proposed that this inverting process can succeed (Raeisi *et al.*, 2012).

D. Experimental implementation of phase-covariant quantum cloning by nitrogen-vacancy defect center in diamond

The economic phase-covariant quantum cloning involves only three states of two-qubit system. Experimentally, we can encode those three states by three energy levels in a specified physical system. The experimental implementation of phase-covariant quantum cloning by this scheme is realized in solid state system (Pan *et al.*, 2011). This solid system is the nitrogen-vacancy (NV) defect center in diamond. The structure of NV center in diamond is that a carbon atom is replaced by a nitrogen atom and additionally a vacancy is located in a nearby lattice site. The NV center is negative charged and can provide three states of the electronic spin one. Those three states correspond to zero magnetic moment ($m_s = 0$) with a 2.87-GHz zero field splitting, two magnetic sub-levels induced by external magnetic field corresponding to $m_s = \pm 1$. The experimental samples of diamond can be bulk or nanodiamond. The electronic spin in NV center of diamond can be individually addressed by using confocal microscopy so that we can control it exactly, however, ensemble of NV centers can also be well controlled. The NV center can be initialized to state $m_s = 0$ polarization by a continuous 532nm laser excitation.

The superposed states of $m_s = 0$ with $m_s = \pm 1$ are prepared by resonating microwaves depending on the duration time determined by their corresponding Rabi oscillations. The microwave radiation is sent out by a copper wire of 20 μm diameter placed with a distance of 20 μm from the NV center. The Rabi oscillations corresponding to different microwave frequencies show that the prepared states are superposed states in quantum mechanics. The resonating frequencies of the controlling microwaves are determined by the electronic-spin-resonating (ESR) spectrum of the NV center obtained by frequency continuously changing. The readout of the electronic state is by Rabi oscillation, the measured value depends on the intensity of the florescence which corresponding to the amplitude of state $m_s = 0$ in the superposed state. The intensity of florescence is measured by single photon counting module connected with a multifunction data acquisition device. The main advantage of the NV center in diamond is its long coherence time which is long enough for spin electronic spin manipulation for various tasks in quantum information processing.

One key point in precisely control the electron spin state is that it does not interact with environmental spin bath mainly constituted by nearby nuclear spins. The fact is that when the electron spin is in state with zero magnetic moment, $m_s = 0$, it does not interact with the nuclear spin. If the electron spin is in either of the $m_s = \pm 1$ states, it is under the influence of the nearby nuclear spin. We may, on the one hand, use this coherent coupling for quantum information purposes, such as to generate entangled state or for quantum memory. On the other hand, it causes decoherence of the quantum state of the electron spin in the NV center. The interaction between the electron spin and a nearby nuclear spin in the NV center can be clearly shown by hyperfine structure in the ESR spectrum.

The general spin Hamiltonian of the NV center consisting of an electron spin, $\mathbf{S}$, coupled with nearby nuclear spins, $\mathbf{I}_k$, is given as,

$$H_{spin} = H_{zf} + H_{eZeeman} + H_{hf} + H_q + H_{nZeeman}, \tag{404}$$

where the terms in spin Hamiltonian describe: the electron spin zero field splitting, $H_{ZF} = \mathbf{S}\bar{D}\mathbf{S}$, the electron Zeeman interaction, $H_{eZeeman} = \beta_e \vec{B}_0 \bar{g}_e \mathbf{S}$, hyperfine interactions between the electron spin and nuclear spins $H_{hf} = \sum_k \mathbf{S}\bar{A}_k \mathbf{I}_k$, the quadrupole interactions for nuclei with $I > 1/2$, $H_q = \sum_{I_k>1} \mathbf{I}_k \bar{P}_k \mathbf{I}_k$, and the nuclear Zeeman interactions, $H_{nZeeman} = -\beta_n \sum_k g_{n,k} \vec{B}_0 \mathbf{I}_k$, also g_e and g_n are the g factors for the electron and nuclei respectively, β_e, β_g are Bohr magnetons for electron and nucleus, $\bar{A}$ and $\bar{P}$ are coupling tensors of hyperfine and quadrupole, and $\vec{B}_0$ is the applied magnetic field.

In implementation of economic phase-covariant quantum cloning, we use four equatorial qubits equivalent to BB84 states. However, according to result of minimal input set, it is also possible to check just three equatorial qubits (Jing *et al.*, 2012). Since only three orthogonal states are involved in the economic phase-covariant cloning, the scheme is to use three physical states $m_s = 0, m_s = \pm 1$ to represent logic states of qubits. In the experimental scheme, the encode scheme is that: $|10\rangle \rightarrow m_s = 0$, $|00\rangle$ and $|01\rangle$ correspond to $m_s = \pm 1$ respectively.

The implementation of phase cloning is in two steps. The first step is the initial state preparation which includes the input state preparation and cloning machine initialization. The experimental realization of this step is to prepare the logic qubits $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)|0\rangle$, which is to prepare physically a superposed state of two involved levels. It is realized by initializing the NV center, applying a $\pi/2$ pulse microwave. The second step of the phase cloning is to realize the quantum cloning transformation. According to the optimal transformation $|00\rangle \rightarrow |00\rangle, |10\rangle \rightarrow \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$, we can realize it by applying another $\pi/2$ pulse microwave. So now the phase quantum cloning is realized experimentally. To readout the result, we can use the combination of two Rabi oscillations to find the exact value of the output state. Experimentally, it is shown that the experimental results are very close with theoretical expectations. In average, the experimental fidelity is about 85.2% which is very close to theoretical optimal bound $1/2 + \sqrt{1/8} \approx 85.4\%$ and is clearly better than the universal quantum cloning. To run all values of the phase parameter, the active controlling of the phase parameter should be performed in experiment. This can also be realized experimentally by using two independently microwave sources.

E. Experimental developments

By quantum circuit method as shown in FIG. 11, the universal cloning is realized by nuclear magnetic resonance (NMR) (Cummins *et al.*, 2002). The phase-covariant cloning is also realized in NMR system with input states ranging from the equator to the polar possessing an arbitrary phase parameter (Du *et al.*, 2005). The UQCM is realized experimentally by single photon with different degrees of freedoms (Huang *et al.*, 2001), stimulated emission with optical fiber amplifier (Fasel *et al.*, 2002). Also in optical system, the UQCM and the NOT gate are realized (Martini *et al.*, 2004). Closely related with optical cloning, the experimental noiseless amplifier for quantum light states is performed (Zavatta *et al.*, 2011). The UQCM realization in cavity QED is proposed in (Milman *et al.*, 2003). Experimental of various cloning machines in one set is performed recently in optics system (Lemr *et al.*, 2012).

Quantum cloning machine can be used for metrology. It is proposed theoretically and shown experimentally with an all-fiber experiment at telecommunications wavelengths that the optimal cloning machine can be used as a radiometer to measure the amount of radiated power (Sanguinetti *et al.*, 2010). The electro-optic quantum memory for light by atoms is demonstrated experimentally and compared with the limit of no-cloning limit (Hetet *et al.*, 2008).

Acknowlegements: This work was supported by "973" program (2010CB922904), grants from Chinese Academy of Sciences, NSFC (11175248) and NFFTBS (J1030310). H.F. would like to thank useful discussions and communications concerning about this topic with V. Buzěk, Kai Chen, Zeng-Bing Chen, I. Cirac, G. M. D'Ariano Jiang-Feng Du, Lu-Ming Duan, Shao-Ming Fei, J. Fiurasek, N. Gisin, Guang-Can Guo, A. Hayashi, Yun-Feng Huang, W. Y. Hwang, H. Imai, Vladimir Korepin, L. C. Kwek, Shu-Shen Li, Hai-Qing Lin, Nai-Le Liu, Seth Lloyd, Gui-Lu Long, Shun-Long Luo, C. Macchieveallo, K. Matsumoto, Xin-Yu Pan, Jian-Wei Pan, Martin Plenio, Vwani Roychowdhury, Xi-Jun Ren, Chang-Pu Sun, Vlatko Vedral, Miki Wadati, Xiang-Bin Wang, Zi-Dan Wang, R. Werner, Ru-Quan Wang, Sheng-Jun Wu, Zheng-Jun Xi, Tao Xiang, Zhao-Xi Xiong, Eli Yablonovitch, Si-Xia Yu, P. Zanardi, Jing Zhang, Zheng-Wei Zhou, Xu-Bo Zou, he also would like to thank continuous support from En-Ge Wang, Yu-Peng Wang, Xin-Cheng Xie, Qi-Kun Xue and Lu Yu. We thank Jun Feng for careful reading this article and Shuai Cui for drawing some pictures.

XII. APPENDIX

For sequential quantum cloning machine of qudits, some detailed results are presented here. We shall provide the explicit form of matrix $V^{[n]i_n}$ for different kinds of sequential UQCM.

A. $N \to M$ sequential UQCM of qubits.

1. When $n = 1$: The upper left corner of $V^{[1]i_1}$ is

$$V^{[1]0} = \begin{pmatrix} \lambda_{[1]1} & 0 \\ 0 & \lambda_{[1]2} \end{pmatrix},\ V^{[1]1} = \begin{pmatrix} 0 & \lambda_{[1]1} \\ \lambda_{[1]2} & 0 \end{pmatrix},$$

while for $\alpha_1 \geq 3$, set $V_{xy}^{[1]i_1} = \frac{1}{\sqrt{2}}\delta_{xy}$.

2. Case $1 < n \leq M - N + m$.

For $1 \leq \alpha_n, \alpha_{n-1} \leq n$,

$$V^{[n]0}_{\alpha_n\alpha_{n-1}} = \delta_{\alpha_n\alpha_{n-1}} \sqrt{\frac{\sum_{k=-m}^{M-m-n} \beta^2_{m(\alpha_{n-1}-1+k)} \frac{C_{M-n}^{m+k}}{C_M^{m+\alpha_{n-1}-1+k}}}{\sum_{k=-m}^{M-m-n+1} \beta^2_{m(\alpha_{n-1}-1+k)} \frac{C_{M-n+1}^{m+k}}{C_M^{m+\alpha_{n-1}-1+k}}}}, \tag{405}$$

otherwise $V^{[n]0}_{\alpha_n\alpha_{n-1}} = \delta_{\alpha_n\alpha_{n-1}} \frac{1}{\sqrt{2}}$.

For $2 \leq \alpha_n \leq (n+1)$, $1 \leq \alpha_{n-1} \leq n$,

$$V^{[n]1}_{\alpha_n\alpha_{n-1}} = \delta_{\alpha_n(\alpha_{n-1}+1)} \sqrt{\frac{\sum_{k=-m}^{M-m-n} \beta^2_{m(\alpha_{n-1}+k)} \frac{C_{M-n}^{m+k}}{C_M^{m+\alpha_{n-1}+k}}}{\sum_{k=-m}^{M-m-n+1} \beta^2_{m(\alpha_{n-1}-1+k)} \frac{C_{M-n+1}^{m+k}}{C_M^{m+\alpha_{n-1}-1+k}}}}, \tag{406}$$

for $\alpha_n = 1, \alpha_{n-1} = n+1$, $V^{[n]1}_{\alpha_n \alpha_{n-1}} = \frac{1}{\sqrt{2}}$, otherwise $V^{[n]1}_{\alpha_n \alpha_{n-1}} = \delta_{\alpha_n \alpha_{n-1}} \frac{1}{\sqrt{2}}$.

3. Case $M - N + m < n \leq M - m$.
   For $1 \leq \alpha_n, \alpha_{n-1} \leq (M - N + m + 1)$,

$$V^{[n]0}_{\alpha_n \alpha_{n-1}} = \delta_{\alpha_n \alpha_{n-1}} \sqrt{\frac{\sum\limits_{k=-m}^{M-m-n} \beta^2_{m(\alpha_{n-1}-1+k)} \frac{C^{m+k}_{M-n}}{C_M^{m+\alpha_{n-1}-1+k}}}{\sum\limits_{k=-m}^{M-m-n+1} \beta^2_{m(\alpha_{n-1}-1+k)} \frac{C^{m+k}_{M-n+1}}{C_M^{m+\alpha_{n-1}-1+k}}}}. \tag{407}$$

   For $2 \leq \alpha_n \leq (M - N + m + 1)$, $1 \leq \alpha_{n-1} \leq (M - N + m)$,

$$V^{[n]1}_{\alpha_n \alpha_{n-1}} = \delta_{\alpha_n (\alpha_{n-1}+1)} \sqrt{\frac{\sum\limits_{k=-m}^{M-m-n} \beta^2_{m(\alpha_{n-1}+k)} \frac{C^{m+k}_{M-n}}{C_M^{m+\alpha_{n-1}+k}}}{\sum\limits_{k=-m}^{M-m-n+1} \beta^2_{m(\alpha_{n-1}-1+k)} \frac{C^{m+k}_{M-n+1}}{C_M^{m+\alpha_{n-1}-1+k}}}}, \tag{408}$$

   otherwise, $V^{[n]1}_{\alpha_n \alpha_{n-1}} = 0$.

4. Case $M - m < n \leq M - 1$.
   (1). For $(m + n + 1 - M) \leq \alpha_n, \alpha_{n-1} \leq (M - N + m + 1)$,

$$V^{[n]0}_{\alpha_n \alpha_{n-1}} = \delta_{\alpha_n \alpha_{n-1}} \sqrt{\frac{\sum\limits_{k=-m}^{M-m-n} \beta^2_{m(\alpha_{n-1}-1+k)} \frac{C^{m+k}_{M-n}}{C_M^{m+\alpha_{n-1}-1+k}}}{\sum\limits_{k=-m}^{M-m-n+1} \beta^2_{m(\alpha_{n-1}-1+k)} \frac{C^{m+k}_{M-n+1}}{C_M^{m+\alpha_{n-1}-1+k}}}}. \tag{409}$$

   For $\alpha_n = m + n - M$, $1 \leq \alpha_{n-1} \leq (M - N + m + 1)$, $V^{[n]0}_{\alpha_M \alpha_{M-1}} = 0$. Otherwise, $V^{[n]0}_{\alpha_n \alpha_{n-1}} = \delta_{\alpha_n \alpha_{n-1}} \frac{1}{\sqrt{2}}$.
   (2). For $(m + n + 1 - M) \leq \alpha_n \leq (M - N + m + 1)$, $(m + n - M) \leq \alpha_{n-1} \leq (M - N + m)$,

$$V^{[n]1}_{\alpha_n \alpha_{n-1}} = \delta_{\alpha_n (\alpha_{n-1}+1)} \sqrt{\frac{\sum\limits_{k=-m}^{M-m-n} \beta^2_{m(\alpha_{n-1}+k)} \frac{C^{m+k}_{M-n}}{C_M^{m+\alpha_{n-1}+k}}}{\sum\limits_{k=-m}^{M-m-n+1} \beta^2_{m(\alpha_{n-1}-1+k)} \frac{C^{m+k}_{M-n+1}}{C_M^{m+\alpha_{n-1}-1+k}}}}. \tag{410}$$

   For $\alpha_n = m + n - M$, $1 \leq \alpha_{n-1} \leq (M - N + m + 1)$, $V^{[n]1}_{\alpha_M \alpha_{M-1}} = 0$. Otherwise, $V^{[n]1}_{\alpha_n \alpha_{n-1}} = \delta_{\alpha_n \alpha_{n-1}} \frac{1}{\sqrt{2}}$.

5. Case $n = M$.
   (1). For $(m + 1) \leq \alpha_M, \alpha_{M-1} \leq (M - N + m + 1)$,

$$V^{[M]0}_{\alpha_M \alpha_{M-1}} = \delta_{\alpha_M \alpha_{M-1}} \sqrt{\frac{\beta^2_{m(\alpha_{M-1}-1-m)}/C_M^{\alpha_{M-1}-1}}{\beta^2_{m(\alpha_{M-1}-1-m)}/C_M^{\alpha_{M-1}-1} + \beta^2_{m(\alpha_{M-1}-m)}/C_M^{\alpha_{M-1}}}}. \tag{411}$$

   For $\alpha_M = m$, $1 \leq \alpha_{M-1} \leq (M - N + m + 1)$, $V^{[M]0}_{\alpha_M \alpha_{M-1}} = 0$. Otherwise, $V^{[M]0}_{\alpha_M \alpha_{M-1}} = \delta_{\alpha_M \alpha_{M-1}} \frac{1}{\sqrt{2}}$.
   (2). For $(m + 1) \leq \alpha_M \leq (M - N + m + 1)$, $m \leq \alpha_{M-1} \leq (M - N + m)$,

$$V^{[M]1}_{\alpha_M \alpha_{M-1}} = \delta_{\alpha_M (\alpha_{M-1}+1)} \sqrt{\frac{\beta^2_{m(\alpha_{M-1}-m)}/C_M^{\alpha_{M-1}}}{\beta^2_{m(\alpha_{M-1}-1-m)}/C_M^{\alpha_{M-1}-1} + \beta^2_{m(\alpha_{M-1}-m)}/C_M^{\alpha_{M-1}}}}. \tag{412}$$

   For $\alpha_M = m$, $1 \leq \alpha_{M-1} \leq (M - N + m + 1)$, $V^{[M]0}_{\alpha_M \alpha_{M-1}} = 0$. Otherwise, $V^{[M]0}_{\alpha_M \alpha_{M-1}} = \delta_{\alpha_M \alpha_{M-1}} \frac{1}{\sqrt{2}}$.

6. Case $n = M + l$.

(1). For $(m+1) \leq \alpha_{M+l} \leq (M-N+m-l+1)$, $(m+2) \leq \alpha_{M+l-1} \leq (M-N+m-l+2)$,

$$V^{[M+l]0}_{\alpha_{M+l}\alpha_{M+l-1}} = \delta_{\alpha_{M+l}(\alpha_{M+l-1}-1)} \sqrt{\frac{\alpha_{M+l-1}-m-1}{M-N-l+1}}. \tag{413}$$

For $\alpha_{M+l} = (M-N+m-l+2)$, $1 \leq \alpha_{M+l-1} \leq (M-N+m+1)$, $V^{[M+l]0}_{\alpha_{M+l}\alpha_{M+l-1}} = 0$. Otherwise $V^{[M+l]0}_{\alpha_{M+l}\alpha_{M+l-1}} = \delta_{\alpha_{M+l}\alpha_{M+l-1}} \frac{1}{\sqrt{2}}$.

(2). For $(m+1) \leq \alpha_{M+l}, \alpha_{M+l-1} \leq (M-N+m-l+1)$,

$$V^{[M+l]1}_{\alpha_{M+l}\alpha_{M+l-1}} = \delta_{\alpha_{M+l}\alpha_{M+l-1}} \sqrt{\frac{M-N-l-\alpha_{M+l-1}+m+2}{M-N-l+1}}. \tag{414}$$

For $\alpha_{M+l} = (M-N+m-l+2)$, $1 \leq \alpha_{M+l-1} \leq (M-N+m+1)$, $V^{[M+l]0}_{\alpha_{M+l}\alpha_{M+l-1}} = 0$. Otherwise $V^{[M+l]0}_{\alpha_{M+l}\alpha_{M+l-1}} = \delta_{\alpha_{M+l}\alpha_{M+l-1}} \frac{1}{\sqrt{2}}$.

Here we have got all the operators $V^{[n]i_n}_{(m)}$ for $0 \leq m \leq N-m$. When $N-m < m \leq N$, one can find that $V^{[n]i_n}_{(m)} = V^{[n]\overline{i_n}}_{(N-m)}$, $\overline{i_n} = i_n + 1\,(\text{mod}2)$.

B. $N \to M$ sequential UQCM of qudits

1. Case $n = 1$.

$$\lambda^{[1]}_{\alpha_1} = \sqrt{\sum_{\boldsymbol{k}=-\boldsymbol{j}'}^{M-N-\boldsymbol{j}'} \beta^2_{\boldsymbol{m}(\boldsymbol{j}'+\boldsymbol{k})} \frac{m_{i_1+1} + j'_{i_1+1} + k_{i_1+1}}{M}},$$

where $\beta_{\boldsymbol{m}\boldsymbol{j}} = \sqrt{\prod_{i=1}^{d} C^{m_i}_{m_i+j_i} / C^{M-N}_{M+d-1}}$.

$$\Gamma^{[1]i_1}_{\alpha_1} = \delta_{\alpha_1 \boldsymbol{j}'}.$$

$$V^{[1]i_1}_{\alpha_1} = \Gamma^{[1]i_1}_{\alpha_1} \lambda^{[1]}_{\alpha_1}.$$

2. Case $1 < n \leq M-1$.

$$\lambda^{[n]}_{\boldsymbol{j}'} = \sqrt{\sum_{\boldsymbol{k}=-\boldsymbol{j}'}^{M-N-\boldsymbol{j}'} \beta^2_{\boldsymbol{m}(\boldsymbol{j}'+\boldsymbol{k})} \prod_{i=1}^{d} C^{j'_i}_{j'_i+k_i+m_i} / C^n_M}.$$

$$\lambda^{[n-1]}_{\boldsymbol{j}"} = \sqrt{\sum_{\overset{'}{k}=-\boldsymbol{j}"}^{M-N-\boldsymbol{j}"} \beta^2_{\boldsymbol{m}(\boldsymbol{j}"+\boldsymbol{k}')} \prod_{i=1}^{d} C^{j"_i}_{j"_i+k'_i+m_i} / C^{n-1}_M}.$$

$$\Gamma^{[n]i_n}_{\boldsymbol{j}"\alpha_n} = \delta_{\alpha_n(\boldsymbol{j}"+\hat{e}_{i_n+1})} \frac{1}{\lambda^{[n-1]}_{\boldsymbol{j}"}} \sqrt{\frac{\boldsymbol{j}"_{i_n+1}+1}{n}}.$$

$$V^{[n]i_n}_{\alpha_n\boldsymbol{j}"} = \delta_{\alpha_n(\boldsymbol{j}"+\hat{e}_{i_n+1})} \sqrt{\frac{\boldsymbol{j}"_{i_n+1}+1}{n}} \frac{\lambda^{[n]}_{\boldsymbol{j}"+\hat{e}_{i_n+1}}}{\lambda^{[n-1]}_{\boldsymbol{j}"}}.$$

3. Case $n = M$.

$$\lambda^{[M]}_{\boldsymbol{j}"} = \beta_{\boldsymbol{m}(\boldsymbol{j}'-\boldsymbol{m})}.$$

$$\lambda^{[M-1]}_{\boldsymbol{j}"} = \sqrt{\sum_{i_M=0}^{d-1} \beta^2_{\boldsymbol{m}(\boldsymbol{j}"-\boldsymbol{m}+\hat{e}_{i_M+1})} \frac{\boldsymbol{j}"_{i_M+1}+1}{M}}.$$

$$\Gamma^{[M]i_M}_{\boldsymbol{j}"\alpha_M} = \delta_{\alpha_M(\boldsymbol{j}"+\hat{e}_{i_M+1})} \frac{1}{\lambda^{[M-1]}_{\boldsymbol{j}"}} \sqrt{\frac{\boldsymbol{j}"_{i_M+1}}{M}}.$$

$$V^{[M]i_M}_{\alpha_M\boldsymbol{j}"} = \delta_{\alpha_M(\boldsymbol{j}"+\hat{e}_{i_M+1})} \frac{\lambda^{[M]}_{\alpha_M}}{\lambda^{[M-1]}_{\boldsymbol{j}"}} \sqrt{\frac{\boldsymbol{j}"_{i_M+1}}{M}}.$$

4. Case $n = M + l$.

$$\lambda^{[M+l]}_{\boldsymbol{j}'} = \sqrt{\sum_{\boldsymbol{k}=\boldsymbol{m}-\boldsymbol{j}'}^{M-N+\boldsymbol{m}-\boldsymbol{j}'} \beta^2_{\boldsymbol{m}(\boldsymbol{j}'-\boldsymbol{m}+\boldsymbol{k})} \prod_{i=1}^{d} C^{k_i}_{j'_i-m_i+k_i} / C^{l}_{M-N}}.$$

$$\lambda^{[M+l-1]}_{\boldsymbol{j}"} = \sqrt{\sum_{\boldsymbol{k}=\boldsymbol{m}-\boldsymbol{j}"}^{M-N+\boldsymbol{m}-\boldsymbol{j}"} \beta^2_{\boldsymbol{m}(\boldsymbol{j}"-\boldsymbol{m}+\boldsymbol{k})} \prod_{i=1}^{d} C^{k'_i}_{j"_i-m_i+k'_i} / C^{l-1}_{M-N}}.$$

$$\Gamma^{[M+1]i_n}_{\boldsymbol{j}"\alpha_n} = \delta_{\alpha_n(\boldsymbol{j}"-\hat{e}_{i_n+1})} \frac{1}{\lambda^{[M+l]}_{\alpha_n}} \sqrt{\frac{j"_{i_n+1}-m_{i_n+1}}{M-N-l+1}}.$$

$$V^{[n]i_n}_{\alpha_n\boldsymbol{j}"} = \delta_{\alpha_n(\boldsymbol{j}"-\hat{e}_{i_n+1})} \sqrt{\frac{j"_{i_n+1}-m_{i_n+1}}{M-N-l+1}}.$$

With the above information, one can build the explicit form of $V^{[n]i_n}$ according to the 2-dimensional case, and the extension is direct.

References

Acín, A., N. Gisin, M. Lluis, and V. Scarani, 2004a, Int. J. Quant. Inf. **2**, 23.
Acín, A., N. Gisin, and V. Scarani, 2003, Quant. Inf. Comput. **3**, 563.
Acín, A., N. Gisin, and V. Scarani, 2004b, Phys. Rev. A **69**, 012309.
Adhikari, S., and B. S. Choudhury, 2006, Phys. Rev. A **74**, 032323.
Adhikari, S., A. S. Majumdar, and N. Nayak, 2008, Phys. Rev. A **77**, 042301.
Adhikari, S., A. K. Pati, I. Chakrabarty, and B. S. Choudhury, 2007, Quant. Inf. Process. **6**, 197.
Albeverio, S., and S. M. Fei, 2000, Eur. Phys. J. B **14**, 669.
Alexanian, M., 2006, Phys. Rev. A **73**, 045801.
Andersen, U. L., V. Josse, and G. Leuchs, 2005, Phys. Rev. Lett. **94**, 240503.
Anselmi, F., A. Chefles, and M. B. Plenio, 2004, New J. Phys. **6**, 164.
Araneda, G., N. Cisternas, O. Jimenez, and A. Delgado, 2012, Phys. Rev. A **86**, 052332.
Audenaert, K., and B. De Moor, 2002, Phys. Rev. A **65**, 030302.
Azuma, K., J. Shimamura, M. Koashi, and N. Imoto, 2005, Phys. Rev. A **72**, 032335.
Bae, J., 2012a, arXiv:1210.3125 .
Bae, J., 2012b, arXiv:1210.2845 .
Bae, J., and A. Acín, 2006, Phys. Rev. Lett. **97**, 030402.
Bae, J., and A. Acin, 2007, Phys. Rev. A **75**, 012334.
Bae, J., and W. Y. Hwang, 2012, arXiv:1204.2313 .
Bae, J., W. Y. Hwang, and Y. D. Han, 2011, Phys. Rev. Lett. **107**, 170403.
Baghbanzadeh, S., and A. T. Rezakhani, 2009, Phys. Lett. A **373**, 821.
Banaszek, K., 2001, Phys. Rev. Lett. **86**, 1366.
Bandyopadhyay, S., P. Boykin, V. Roychowdhury, and F. Vatan, 2002, Algorithmica **34**, 512.
Barenco, A., C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, 1995, Phys. Rev. A **52**, 3457.
Barnum, H., J. Barrett, M. Leifer, and A. Wilce, 2007, Phys. Rev. Lett. **99**, 240501.
Barnum, H., C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, 1996, Phys. Rev. Lett. **76**, 2818.
Bartkiewicz, K., K. Lemr, A. Černoch, J. Soubusta, and A. Miranowicz, 2012, arXiv:1206.0144 .
Bartkiewicz, K., and A. Miranowicz, 2010, Phys. Rev. A **82**, 042330.
Bartkiewicz, K., and A. Miranowicz, 2012, Phys. Scrip. **T147**, 014003.
Bartkiewicz, K., A. Miranowicz, and S. K. Ozdemir, 2009, Phys. Rev. A **80**, 032306.
Bartuskova, L., M. Dusek, A. Cernoch, J. Soubusta, and J. Fiurasek, 2007, Phys. Rev. Lett. **99**, 120505.
Bechmann-Pasquinucci, H., and N. Gisin, 1999, Phys. Rev. A **59**, 4238.
Bechmann-Pasquinucci, H., and W. Tittel, 2000, Phys. Rev. A **61**, 062308.
Bell, J. S., 1964, Phys. **1**, 195.
Bennett, C. H., 1992, Phys. Rev. Lett. **68**, 3121.
Bennett, C. H., and G. Brassard, 1984, in *In Proceeding if IEEE Int. Conf. on Computers, Systems, and Signal Processings (Bangalore, India, 1984)* (IEEE, New York), pp. 175–179.
Bennett, C. H., G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, 1993, Phys. Rev. Lett. **70**, 1895.
Bennett, C. H., G. Brassard, and N. D. Mermin, 1992, Phys. Rev. Lett. **68**, 557.
Bisio, A., G. Chiribella, G. M. D'Ariano, S. Facchini, and P. Perinotti, 2010, Phys. Rev. A **81**, 032324.
Bisio, A., G. M. D'Ariano, P. Perinotti, and M. Sedlak, 2011, Phys. Rev. A **84**, 042330.
Bourennane, M., A. Karlsson, and G. Björk, 2001, Phys. Rev. A **64**, 012306.
Bradler, K., 2011, IEEE Trans. Inf. Theory **57**, 5497.
Bradler, K., and R. Jauregui, 2008, Phys. Rev. A **77**, 042302.
Braunstein, S. L., N. J. Cerf, S. Iblisdir, P. van Loock, and S. Massar, 2001a, Phys. Rev. Lett. **86**, 4938.
Braunstein, S. L., C. A. Fuchs, and H. J. Kimble, 2000, J. Mod. Optic. **47**, 267.
Braunstein, S. L., and P. van Loock, 2005, Rev. Mod. Phys. **77**, 513.
Braunstein, S. L., V. Bužek, and M. Hillery, 2001b, Phys. Rev. A **63**, 052313.
Brougham, T., E. Andersson, and S. M. Barnett, 2006, Phys. Rev. A **73**, 062319.
Bruß, D., 1998, Phys. Rev. Lett. **81**, 3018.
Bruß, D., J. Calsamiglia, and N. Lütkenhaus, 2001, Phys. Rev. A **63**, 042308.
Bruß, D., M. Cinchetti, G. Mauro D'Ariano, and C. Macchiavello, 2000a, Phys. Rev. A **62**, 012302.
Bruß, D., G. M. D'Ariano, C. Macchiavello, and M. F. Sacchi, 2000b, Phys. Rev. A **62**, 062302.
Bruß, D., D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, 1998a, Phys. Rev. A **57**, 2368.
Bruß, D., A. Ekert, and C. Macchiavello, 1998b, Phys. Rev. Lett. **81**, 2598.
Bruß, D., and C. Macchiavello, 1999, Phys. Lett. A **253**, 249 .
Bruß, D., and C. Macchiavello, 2002, Phys. Rev. Lett. **88**, 127901.
Bruß, D., and C. Macchiavello, 2003, Found. Phys. **33**, 1617.
Bub, J., 2001, Phys. Rev. A **63**, 032309.
Buscemi, F., G. M. D'Ariano, and C. Macchiavello, 2005, Phys. Rev. A **71**, 042327.
Buscemi, F., G. M. D'Ariano, and C. Macchiavello, 2007, J. Opt. Soc. Am. B **24**, 363.

Buscemi, F., G. M. D'Ariano, C. Macchiavello, and P. Perinotti, 2006, Phys. Rev. A **74**, 042309.
Buscemi, F., G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, 2003, Phys. Lett. A **314**, 374 .
Bužek, V., S. L. Braunstein, M. Hillery, and D. Bruß, 1997a, Phys. Rev. A **56**, 3446.
Bužek, V., and M. Hillery, 1996, Phys. Rev. A **54**, 1844.
Bužek, V., and M. Hillery, 1998, Phys. Rev. Lett. **81**, 5003.
Bužek, V., and M. Hillery, 1999, in *QUANTUM COMPUTING AND QUANTUM COMMUNICATIONS*, edited by C. Williams, volume 1509 of *LECTURE NOTES IN COMPUTER SCIENCE*, pp. 235–246.
Bužek, V., and M. Hillery, 2000, J. Mod. Optic. **47**, 211.
Bužek, V., M. Hillery, and R. Bednik, 1998, Acta Phys. Slovaca **48**, 177.
Bužek, V., M. Hillery, and R. F. Werner, 1999, Phys. Rev. A **60**, 2626(R).
Bužek, V., V. Vedral, M. B. Plenio, P. L. Knight, and M. Hillery, 1997b, Phys. Rev. A **55**, 3327.
Caminati, M., F. De Martini, R. Perris, F. Sciarrino, and V. Secondi, 2006, Phys. Rev. A **74**, 062304.
Cao, Z. L., and W. Song, 2004, Phys. Lett. A **325**, 309.
Carlini, A., and M. Sasaki, 2003, Phys. Rev. A **68**, 042327.
Caves, C. M., 1982, Phys. Rev. D **26**, 1817.
Cerf, N. J., 1998, Acta Phys. Slovaca **48**, 115.
Cerf, N. J., 2000a, J. Mod. Optic. **47**, 187 .
Cerf, N. J., 2000b, Phys. Rev. Lett. **84**, 4497.
Cerf, N. J., M. Bourennane, A. Karlsson, and N. Gisin, 2002a, Phys. Rev. Lett. **88**, 127902.
Cerf, N. J., T. Durt, and N. Gisin, 2002b, J. Mod. Optic. **49**, 1355 .
Cerf, N. J., and J. Fiurášek, 2006 (Elsevier), volume 49 of *Progress in Optics*, pp. 455 – 545.
Cerf, N. J., and P. Grangier, 2007, J. Opt. Soc. Am. B **24**, 324.
Cerf, N. J., and S. Iblisdir, 2000, Phys. Rev. A **62**, 040301(R).
Cerf, N. J., and S. Iblisdir, 2001a, Phys. Rev. A **64**, 032307.
Cerf, N. J., and S. Iblisdir, 2001b, Phys. Rev. Lett. **87**, 247903.
Cerf, N. J., S. Iblisdir, and G. Van Assche, 2002c, Eur. Phys. J. D **18**, 211.
Cerf, N. J., A. Ipe, and X. Rottenberg, 2000, Phys. Rev. Lett. **85**, 1754.
Cerf, N. J., O. Krüger, P. Navez, R. F. Werner, and M. M. Wolf, 2005, Phys. Rev. Lett. **95**, 070501.
Cerf, N. J., M. Lévy, and G. V. Assche, 2001, Phys. Rev. A **63**, 052311.
Cernoch, A., L. Bartuskova, J. Soubusta, M. Jezek, J. Fiurasek, and M. Dusek, 2006, Phys. Rev. A **74**, 042327.
Cernoch, A., J. Soubusta, L. Celechovska, M. Dusek, and J. Fiurasek, 2009, Phys. Rev. A **80**, 062306.
Chefles, A., and S. M. Barnett, 1998, J. Phys. A-Math. Gen. **31**, 10097.
Chefles, A., and S. M. Barnett, 1999, Phys. Rev. A **60**, 136.
Chefles, A., C. R. Gilson, and S. M. Barnett, 2001, Phys. Rev. A **63**, 032314.
Chen, H. W., D. W. Lu, B. Chong, G. Qin, X. Y. Zhou, X. H. Peng, and J. F. Du, 2011, Phys. Rev. Lett. **106**, 180404.
Chen, H. W., X. Y. Zhou, D. Suter, and J. F. Du, 2007, Phys. Rev. A **75**, 012317.
Chen, H. X., and J. Zhang, 2007, Phys. Rev. A **75**, 022306.
Chen, L., and Y. X. Chen, 2007a, Quant. Inf. Comput. **7**, 716.
Chen, L., and Y. X. Chen, 2007b, Phys. Rev. A **75**, 062322.
Chen, Y. X., and D. Yang, 2001a, Phys. Rev. A **64**, 064303.
Chen, Y. X., and D. Yang, 2001b, Phys. Rev. A **65**, 022320.
Chiara, G. D., R. Fazio, C. Macchiavello, S. Montangero, and G. M. Palma, 2004, Phys. Rev. A **70**, 062308.
Chiribella, G., G. M. D'Ariano, C. Macchiavello, P. Perinotti, and F. Buscemi, 2007, Phys. Rev. A **75**, 012315.
Chiribella, G., G. M. D'Ariano, and P. Perinotti, 2008, Phys. Rev. Lett. **101**, 180504.
Chiribella, G., G. M. D'Ariano, P. Perinotti, and N. J. Cerf, 2005, Phys. Rev. A **72**, 042336.
Cochrane, P. T., T. C. Ralph, and A. Dolińska, 2004, Phys. Rev. A **69**, 042313.
Coffman, V., J. Kundu, and W. K. Wootters, 2000, Phys. Rev. A **61**, 052306.
Collins, D., N. Linden, and S. Popescu, 2001, Phys. Rev. A **64**, 032302.
Cummins, H. K., C. Jones, A. Furze, N. F. Soffe, M. Mosca, J. M. Peach, and J. A. Jones, 2002, Phys. Rev. Lett. **88**, 187901.
Cwiklinski, P., M. Horodecki, and M. Studzinski, 2012, Phys. Lett. A **376**, 2178.
Daffertshofer, A., A. R. Plastino, and A. Plastino, 2002, Phys. Rev. Lett. **88**, 210601.
Dang, G. F., and H. Fan, 2007, Phys. Rev. A **76**, 022323.
Dang, G. F., and H. Fan, 2008, J. Phys. A-Math. Theor. **41**, 155303.
D'Ariano, G. M., F. De Martini, and M. F. Sacchi, 2001, Phys. Rev. Lett. **86**, 914.
D'Ariano, G. M., and P. Lo Presti, 2001, Phys. Rev. A **64**, 042308.
D'Ariano, G. M., and C. Macchiavello, 2003, Phys. Rev. A **67**, 042306.
D'Ariano, G. M., C. Macchiavello, and P. Perinotti, 2005a, Phys. Rev. A **72**, 042327.
D'Ariano, G. M., C. Macchiavello, and P. Perinotti, 2005b, Phys. Rev. Lett. **95**, 060503.
D'Ariano, G. M., and P. Perinotti, 2009, Phys. Lett. A **373**, 2416.
D'Ariano, G. M., P. Perinotti, and M. F. Sacchi, 2006, New J. Phys. **8**, 99.
Dasgupta, S., and G. S. Agarwal, 2001, Phys. Rev. A **64**, 022315.
De Angelis, T., E. Nagali, F. Sciarrino, and F. De Martini, 2007, Phys. Rev. Lett. **99**, 193601.
De Chiara, G., R. Fazio, C. Macchiavello, S. Montangero, and G. M. Palma, 2004, Phys. Rev. A **70**, 062308.
De Martini, F., V. Mussi, and F. Bovino, 2000, Opt. Commun. **179**, 581.

De Martini, F., V. Bužek, F. Sciarrino, and C. Sias, 2002, Nature **419**, 815.
Delgado, Y., L. Lamata, J. Leon, D. Salgado, and E. Solano, 2007, Phys. Rev. Lett. **98**, 150502.
Demkowicz-Dobrzanski, R., M. Kus, and K. Wodkiewicz, 2004, Phys. Rev. A **69**, 012301.
Derka, R., V. Buzěk, and A. K. Ekert, 1998, Phys. Rev. Lett. **80**, 1571.
Deuar, P., and W. J. Munro, 2000a, Phys. Rev. A **61**, 010306(R).
Deuar, P., and W. J. Munro, 2000b, Phys. Rev. A **61**, 062304.
Deuar, P., and W. J. Munro, 2000c, Phys. Rev. A **62**, 042304.
Di Franco, C., M. Paternostro, G. M. Palma, and M. S. Kim, 2007, Phys. Rev. A **76**, 042316.
Dieks, D., 1982, Phys. Lett. A **92**, 271 .
Dong, Y. L., X. B. Zou, and G. C. Guo, 2008, Phys. Rev. A **77**, 034304.
Du, J. F., T. Durt, P. Zou, H. Li, L. C. Kwek, C. H. Lai, C. H. Oh, and A. Ekert, 2005, Phys. Rev. Lett. **94**, 040505.
Duan, L. M., and G. C. Guo, 1998a, Phys. Rev. Lett. **80**, 4999.
Duan, L. M., and G. C. Guo, 1998b, Phys. Lett. A **243**, 261 .
Duan, L. M., and G. C. Guo, 1999, Commun. Theor. Phys. **31**, 223.
Dür, W., 2001, Phys. Rev. A **63**, 020303.
Dür, W., and J. I. Cirac, 2000, J. Mod. Optic. **47**, 247.
Durt, T., and J. F. Du, 2004, Phys. Rev. A **69**, 062316.
Durt, T., J. Fiurášek, and N. J. Cerf, 2005, Phys. Rev. A **72**, 052322.
Durt, T., and B. Nagler, 2003, Phys. Rev. A **68**, 042323.
Durt, T., and J. Van de Putte, 2011, Int. J. Quant. Inf. **9**, 915.
Eisert, J., K. Jacobs, P. Papadopoulos, and M. B. Plenio, 2000, Phys. Rev. A **62**, 052317.
Ekert, A., and R. Jozsa, 1996, Rev. Mod. Phys. **68**, 733.
Ekert, A. K., 1991, Phys. Rev. Lett. **67**, 661.
Englert, B. G., and Y. Aharonov, 2001, Phys. Lett. A **284**, 1.
Fan, H., 2003, Phys. Rev. A **68**, 054301.
Fan, H., 2004, Phys. Rev. Lett. **92**, 177905.
Fan, H., H. Imai, K. Matsumoto, and X. B. Wang, 2003, Phys. Rev. A **67**, 022317.
Fan, H., V. Korepin, and V. Roychowdhury, 2004, Phys. Rev. Lett. **93**, 227203.
Fan, H., B. Y. Liu, and K. J. Shi, 2007, Quant. Inf. Comput. **7**, 551.
Fan, H., K. Matsumoto, and M. Wadati, 2001a, Phys. Rev. A **64**, 064301.
Fan, H., K. Matsumoto, X. B. Wang, and M. Wadati, 2001b, Phys. Rev. A **65**, 012304.
Fan, H., G. Weihs, K. Matsumoto, and H. Imai, 2002, Phys. Rev. A **66**, 024307.
Fang, B. L., Q. M. Song, and L. Ye, 2011, Phys. Rev. A **83**, 042309.
Fang, B. L., T. Wu, and L. Ye, 2012a, Europhys. Lett. **97**, 60002.
Fang, B. L., T. Wu, and L. Ye, 2012b, Quant. Inf. Comput. **12**, 334.
Fang, B. L., and L. Ye, 2010, Phys. Lett. A **374**, 1966.
Fang, M., Y. M. Liu, J. Liu, S. H. Shi, and Z. J. Zhang, 2006, Commun. Theor. Phys. **46**, 849.
Fasel, S., N. Gisin, G. Ribordy, V. Scarani, and H. Zbinden, 2002, Phys. Rev. Lett. **89**, 107901.
Feng, Y., R. Y. Duan, and Z. F. Ji, 2005, Phys. Rev. A **72**, 012313.
Fenyes, A., 2012, J. Math. Phys. **53**, 012902.
Filip, R., 2004a, Phys. Rev. A **69**, 032309.
Filip, R., 2004b, Phys. Rev. A **69**, 052301.
Filip, R., J. Fiurášek, and P. Marek, 2004, Phys. Rev. A **69**, 012314.
Fiurasek, J., and N. J. Cerf, 2007, Phys. Rev. A **75**, 052335.
Fiurasek, J., and N. J. Cerf, 2008, Phys. Rev. A **77**, 052308.
Fiurášek, J., 2001a, Phys. Rev. A **64**, 062310.
Fiurášek, J., 2001b, Phys. Rev. Lett. **86**, 4942.
Fiurášek, J., 2003, Phys. Rev. A **67**, 052314.
Fiurášek, J., 2004, Phys. Rev. A **70**, 032308.
Fiurášek, J., N. J. Cerf, and E. S. Polzik, 2004, Phys. Rev. Lett. **93**, 180501.
Fiurášek, J., R. Filip, and N. J. Cerf, 2005, Quant. Inf. Comput. **5**, 583.
Fiurášek, J., S. Iblisdir, S. Massar, and N. J. Cerf, 2002, Phys. Rev. A **65**, 040302(R).
Frowis, F., and W. Dür, 2012, Phys. Rev. Lett. **109**, 170401.
Fuchs, C. A., N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, 1997, Phys. Rev. A **56**, 1163.
Fuchs, C. A., and A. Peres, 1996, Phys. Rev. A **53**, 2038.
Galvao, E. F., and L. Hardy, 2000, Phys. Rev. A **62**, 022301.
Gedik, Z., and B. Çakmak, 2012, arXiv:1203.3054 .
Ghiu, I., 2003, Phys. Rev. A **67**, 012323.
Ghiu, I., and A. Karlsson, 2005, Phys. Rev. A **72**, 032331.
Ghosh, S., G. Kar, and A. Roy, 1999, Phys. Lett. A **261**, 17 .
Ghosh, S., G. Kar, and A. Roy, 2004, Phys. Rev. A **69**, 052312.
Ghosh, S., G. Kar, A. Roy, A. Sen(De), and U. Sen, 2001, Phys. Rev. Lett. **87**, 277902.
Gisin, N., 1998, Phys. Lett. A **242**, 1 .
Gisin, N., and B. Huttner, 1997, Phys. Lett. A **228**, 13.

Gisin, N., and S. Massar, 1997, Phys. Rev. Lett. **79**, 2153.
Gisin, N., and S. Popescu, 1999, Phys. Rev. Lett. **83**, 432.
Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden, 2002, Rev. Mod. Phys. **74**, 145.
Goldenberg, L., and L. Vaidman, 1996, Phys. Rev. Lett. **77**, 3265.
Gottesman, D., 1998, Phys. Rev. A **57**, 127.
Griffiths, R. B., and C. S. Niu, 1997, Phys. Rev. A **56**, 1173.
Grosshans, F., and N. J. Cerf, 2004, Phys. Rev. Lett. **92**, 047905.
Grosshans, F., and P. Grangier, 2001, Phys. Rev. A **64**, 010301.
Grosshans, F., and P. Grangier, 2002, Phys. Rev. Lett. **88**, 057902.
Guta, M., and K. Matsumoto, 2006, Phys. Rev. A **74**, 032305.
Han, Y. D., J. Bae, X. B. Wang, and W. Y. Hwang, 2010, Phys. Rev. A **82**, 062318.
Hardy, L., and D. D. Song, 1999, Phys. Lett. A **259**, 331 .
Hayashi, A., M. Horibe, and T. Hashimoto, 2005, Phys. Rev. A **71**, 052331.
Hayden, P., R. Jozsa, D. Petz, and A. Winter, 2004, Commun. Math. Phys. **246**, 359.
Herbert, N., 1982, Found. Phys. **12**, 1171.
Hetet, G., J. J. Longdell, A. L. Alexander, P. K. Lam, and M. J. Sellars, 2008, Phys. Rev. Lett. **100**, 023601.
Hillery, M., and V. Bužek, 1997, Phys. Rev. A **56**, 1212.
Holevo, A. S., 1982, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam).
Horodecki, M., P. Horodecki, and R. Horodecki, 1996, Phys. Lett. A **223**, 1 .
Horodecki, M., P. Horodecki, R. Horodecki, and M. Piani, 2006, Int. J. Quant. Inf. **4**, 105.
Horodecki, M., and R. Horodecki, 1998, Phys. Lett. A **244**, 473.
Horodecki, R., P. Horodecki, M. Horodecki, and K. Horodecki, 2009, Rev. Mod. Phys. **81**, 865.
Hu, G. Y., W. H. Zhang, and L. Ye, 2010, Opt. Commun. **283**, 200.
Hu, J. Z., Z. W. Yu, and X. B. Wang, 2009, Eur. Phys. J. D **51**, 381.
Huang, Y. F., W. L. Li, C. F. Li, Y. S. Zhang, Y. K. Jiang, and G. C. Guo, 2001, Phys. Rev. A **64**, 012315.
Iblisdir, S., A. Acín, N. J. Cerf, R. Filip, J. Fiurášek, and N. Gisin, 2005a, Phys. Rev. A **72**, 042328.
Iblisdir, S., A. Acín, and N. Gisin, 2005b, arXiv:quant-ph/0505152v1 .
Irvine, W. T. M., A. Lamas Linares, M. J. A. de Dood, and D. Bouwmeester, 2004, Phys. Rev. Lett. **92**, 047902.
Ishizaka, S., and T. Hiroshima, 2008, Phys. Rev. Lett. **101**, 240501.
Janzing, D., and B. Steudel, 2007, Phys. Rev. A **75**, 022309.
Ji, Z. F., Y. Feng, and M. S. Ying, 2005, Phys. Rev. A **72**, 032324.
Jiang, M. M., and S. X. Yu, 2010a, J. Math. Phys. **51**, 052306.
Jiang, M. M., and S. X. Yu, 2010b, Chin. Phys. Lett. **27**, 010303.
Jimenez, O., J. Bergou, and A. Delgado, 2010a, Phys. Rev. A **82**, 062307.
Jimenez, O., L. Roa, and A. Delgado, 2010b, Phys. Rev. A **82**, 022328.
Jing, L., Y. N. Wang, H. D. Shi, L. Z. Mu, and H. Fan, 2012, Phys. Rev. A **86**, 062315.
Jochym-O'Connor, T., K. Bradler, and M. M. Wilde, 2011, J. Phys. A-Math. Theor. **44**, 415306.
Josza, R., 1994, J. Mod. Optic. **41**, 2315.
Kalev, A., and I. Hen, 2008, Phys. Rev. Lett. **100**, 210502.
Karimipour, V., A. Bahraminasab, and S. Bagherinezhad, 2002, Phys. Rev. A **65**, 052331.
Karimipour, V., and A. T. Rezakhani, 2002, Phys. Rev. A **66**, 052111.
Karpov, E., P. Navez, and N. J. Cerf, 2005, Phys. Rev. A **72**, 042314.
Kay, A., D. Kaszlikowski, and R. Ramanathan, 2009, Phys. Rev. Lett. **103**, 050501.
Kay, A., R. Ramanathan, and D. Kaszlikowski, 2012, arXiv:1208.5574 .
Kazakov, A. Y., 2010, Int. J. Quant. Inf. **8**, 435.
Kempe, J., C. Simon, and G. Weihs, 2000, Phys. Rev. A **62**, 032302.
Keyl, M., and R. F. Werner, 1999, J. Math. Phys. **40**, 3283.
Khan, I. A., and J. C. Howell, 2003, Phys. Rev. A **70**, 010303(R).
Khan, I. A., and J. C. Howell, 2004, Quant. Inf. Comput. **4**, 114.
Kimura, G., H. Tanaka, and M. Ozawa, 2006, Phys. Rev. A **73**, 050301(R).
Kitaev, A. Y., 2001, Phys. USP. **44**, 131.
Koashi, M., and N. Imoto, 1996, Phys. Rev. Lett. **77**, 2137.
Koashi, M., and N. Imoto, 1998, Phys. Rev. Lett. **81**, 4264.
Koashi, M., and N. Imoto, 2002, Phys. Rev. A **66**, 022318.
Kocsis, S., G. Y. Xiang, T. C. Ralph, and G. J. Pryde, 2013, Nat. Phys. **9**, 23.
Koike, S., H. Takahashi, H. Yonezawa, N. Takei, S. L. Braunstein, T. Aoki, and A. Furusawa, 2006, Phys. Rev. Lett. **96**, 060504.
Kraus, B., N. Gisin, and R. Renner, 2005, Phys. Rev. Lett. **95**, 080501.
Kretschmann, D., D. Schlingemann, and R. F. Werner, 2008, IEEE Trans. Inf. Theory **54**, 1708.
Kwek, L. C., C. H. Oh, X. B. Wang, and Y. Yeo, 2000, Phys. Rev. A **62**, 052313.
Lamas-Linares, A., C. Simon, J. C. Howell, and D. Bouwmeester, 2002, Science **296**, 712.
Lamata, L., J. Leon, D. Perez-Garcia, D. Salgado, and E. Solano, 2008, Phys. Rev. Lett. **101**, 180506.
Lamoureux, L. P., and N. J. Cerf, 2005, Quant. Inf. Comput. **5**, 32.
Lamoureux, L. P., P. Navez, J. Fiurášek, and N. J. Cerf, 2004, Phys. Rev. A **69**, 040301(R).

Leifer, M. S., 2006, Phys. Rev. A **74**, 042310.
Lemr, K., K. Bartkiewicz, A. Cernoch, J. Soubusta, and A. Miranowicz, 2012, Phys. Rev. A **85**, 050307(R).
Levente, S., K. Matyas, A. Peter, and J. Jozsef, 2010, Phys. Rev. A **81**, 032323.
Li, D. C., and Z. Y. Shen, 2009, Int. J. Theor. Phys. **48**, 2777.
Li, D. F., X. R. Li, H. T. Huang, and X. X. Li, 2005a, Int. J. Quant. Inf. **3**, 551.
Li, D. F., X. R. Li, H. T. Huang, and X. X. Li, 2005b, J. Math. Phys. **46**, 082102.
Li, L. J., and D. W. Qiu, 2007, Phys. Lett. A **362**, 143.
Li, L. J., D. W. Qiu, L. Z. Li, L. H. Wu, and X. F. Zou, 2009, J. Phys. A-Math. Theor. **42**, 175302.
Li, Y. L., J. Feng, B. L. Liang, and Y. F. Yu, 2007, Int. J. Theor. Phys. **46**, 2599.
Lindblad, G., 1975, Commun. Math. Phys. **40**, 147.
Lindblad, G., 1999, Lett. Math. Phys. **47**, 189.
Lo, H. K., and H. F. Chau, 1999, Science **283**, 2050.
van Loock, P., and S. L. Braunstein, 2000, Phys. Rev. Lett. **84**, 3482.
van Loock, P., and S. L. Braunstein, 2001, Phys. Rev. Lett. **87**, 247901.
Luo, S. L., 2010a, Phys. Lett. A **374**, 1350.
Luo, S. L., 2010b, Lett. Math. Phys. **92**, 143.
Luo, S. L., N. Li, and X. L. Cao, 2009, Phys. Rev. A **79**, 054305.
Luo, S. L., and W. Sun, 2010, Phys. Rev. A **82**, 012338.
Ma, P. C., and Y. B. Zhan, 2009, Commun. Theor. Phys. **51**, 57.
Ma, P. C., Y. B. Zhan, and L. L. Zhang, 2009, Int. J. Mod. Phys. B **23**, 3231.
Ma, Z. Q., 2007, *Group Theory for Physicists, p122-131, p353-364* (World Scientific,Singapore).
Macchiavello, C., 2003, Phys. Rev. A **67**, 062302.
Maccone, L., 2006, Phys. Rev. A **73**, 042307.
Martini, F. D., D. Pelliccia, and F. Sciarrino, 2004, Phys. Rev. Lett. **92**, 067901.
Martini, F. D., and F. Sciarrino, 2012, Rev. Mod. Phys. **84**, 1765.
Masanes, L., A. Acin, and N. Gisin, 2006, Phys. Rev. A **73**, 012112.
Massar, S., 2000, Phys. Rev. A **62**, 040101(R).
Massar, S., and S. Popescu, 1995, Phys. Rev. Lett. **74**, 1259.
Mayer, D., 2001, J. ACM **48**, 351.
Mendonca, P. E. M. F., A. Gilchrist, and A. C. Doherty, 2008, Phys. Rev. A **78**, 012319.
Meng, F. Y., and A. D. Zhu, 2009, J. Mod. Optic. **56**, 1255.
Milman, P., H. Ollivier, and J. M. Raimond, 2003, Phys. Rev. A **67**, 012314.
Mishra, D. K., 2012, Opt. Commun. **285**, 1560.
Miyadera, T., and H. Imai, 2006a, Phys. Rev. A **74**, 064302.
Miyadera, T., and H. Imai, 2006b, Phys. Rev. A **74**, 024101.
Modi, K., A. Brodutch, H. Cable, T. Paterek, and V. Vedral, 2012, Rev. Mod. Phys. **84**, 1655.
Mor, T., 1998, Phys. Rev. Lett. **80**, 3137.
Mor, T., and D. R. Terno, 1999, Phys. Rev. A **60**, 4341.
Murao, M., D. Jonathan, M. B. Plenio, and V. Vedral, 1999, Phys. Rev. A **59**, 156.
Murao, M., M. B. Plenio, and V. Vedral, 2000, Phys. Rev. A **61**, 032311.
Murao, M., and V. Vedral, 2001, Phys. Rev. Lett. **86**, 352.
Nagali, E., T. De Angelis, F. Sciarrino, and F. De Martini, 2007, Phys. Rev. A **76**, 042126.
Nagali, E., D. Giovannini, L. Marrucci, S. Slussarenko, E. Santamato, and F. Sciarrino, 2010, Phys. Rev. Lett. **105**, 073602.
Nagali, E., L. Sansoni, F. Sciarrino, F. De Martini, L. Marrucci, B. Piccirillo, E. Karimi, and E. Santamato, 2009, Nat. Photonics **3**, 720.
Nagy, G., 2009, Rep. Math. Phys. **63**, 447.
Namiki, R., 2011, Phys. Rev. A **83**, 040302(R).
Navez, P., and N. J. Cerf, 2003, Phys. Rev. A **68**, 032313.
Nha, H., and H. J. Carmichael, 2005, Phys. Rev. A **71**, 032336.
Niederberger, A., V. Scarani, and N. Gisin, 2005, Phys. Rev. A **71**, 042316.
Nielsen, M. A., and I. C. Chuang, 2000, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge).
Nikolopoulos, G. M., and G. Alber, 2005, Phys. Rev. A **72**, 032320.
Nikolopoulos, G. M., K. S. Ranade, and G. Alber, 2006, Phys. Rev. A **73**, 032325.
Niu, C. S., and R. B. Griffiths, 1998, Phys. Rev. A **58**, 4377.
Niu, C. S., and R. B. Griffiths, 1999, Phys. Rev. A **60**, 2764.
Niu, X. F., 2009, Int. J. Theor. Phys. **48**, 2599.
Nuida, K., G. Kimura, and T. Miyadera, 2010, J. Math. Phys. **51**, 093505.
Olivares, S., and M. G. A. Paris, 2008, Eur. Phys. J.-Spec. Top. **160**, 319.
Olivares, S., M. G. A. Paris, and U. L. Andersen, 2006, Phys. Rev. A **73**, 062330.
Osborne, T. J., and F. Verstraete, 2006, Phys. Rev. Lett. **96**, 220503.
Ou, Y. C., and H. Fan, 2007, Phys. Rev. A **75**, 062308.
Ou, Y. C., H. Fan, and S. M. Fei, 2008, Phys. Rev. A **78**, 012311.
Owari, M., and M. Hayashi, 2006, Phys. Rev. A **74**, 032108.

Ozdemir, S. K., K. Bartkiewicz, Y. X. Liu, and A. Miranowicz, 2007, Phys. Rev. A **76**, 042325.
Pan, J. W., Z. B. Chen, C. Y. Lu, H. Weinfurter, A. Zeilinger, and M. Zukowski, 2012, Rev. Mod. Phys. **84**, 777.
Pan, X. Y., G. Q. Liu, L. L. Yang, and H. Fan, 2011, Appl. Phys. Lett. **99**, 051113.
Pang, S. S., S. J. Wu, and Z. B. Chen, 2011, Phys. Rev. A **84**, 062313.
Pati, A. K., 1999, Phys. Rev. Lett. **83**, 2849.
Pati, A. K., 2000, Phys. Rev. A **61**, 022308.
Pati, A. K., and S. L. Braunstein, 2000, Nature **404**, 164 .
Pawlowski, M., and C. Brukner, 2009, Phys. Rev. Lett. **102**, 030403.
Pelliccia, D., V. Schettini, F. Sciarrino, C. Sias, and F. De Martini, 2003, Phys. Rev. A **68**, 042306.
Peres, A., 1995, *Quantum Theory: Concepts and Methods* (Springer).
Peres, A., 1996a, Phys. Rev. Lett. **77**, 3264.
Peres, A., 1996b, Phys. Rev. Lett. **77**, 1413.
Peres, A., and W. K. Wootters, 1991, Phys. Rev. Lett. **66**, 1119.
Piani, M., P. Horodecki, and R. Horodecki, 2008, Phys. Rev. Lett. **100**, 090502.
Prevedel, R., G. Cronenberg, M. S. Tame, M. Paternostro, P. Walther, M. S. Kim, and A. Zeilinger, 2009, Phys. Rev. Lett. **103**, 020503.
Qiu, D. W., 2002, Phys. Rev. A **65**, 052329.
Qiu, D. W., 2006, J. Phys. A-Math. Gen. **39**, 5135.
Qiu, D. W., 2008, Phys. Rev. A **77**, 012328.
Raeisi, S., W. Tittel, and C. Simon, 2012, Phys. Rev. Lett. **108**, 120404.
Rastegin, A. E., 2002, Phys. Rev. A **66**, 042304.
Rastegin, A. E., 2003a, Phys. Rev. A **68**, 032303.
Rastegin, A. E., 2003b, Phys. Rev. A **67**, 012305.
Rastegin, A. E., 2010, Quant. Inf. Comput. **10**, 971.
Raynal, P., and N. Lutkenhaus, 2005, Phys. Rev. A **72**, 022342.
Reck, M., A. Zeilinger, H. J. Bernstein, and P. Bertani, 1994, Phys. Rev. Lett. **73**, 58.
Reimpell, M., and R. F. Werner, 2007, Phys. Rev. A **75**, 062334.
Ren, X., Y. Xiang, and H. Fan, 2011, Eur. Phys. J. D **65**, 621.
Renes, J. M., 2004, Phys. Rev. A **70**, 052314.
Rezakhani, A., S. Siadatnejad, and A. Ghaderi, 2005, Phys. Lett. A **336**, 278 .
Ricci, M., F. Sciarrino, N. J. Cerf, R. Filip, J. Fiurášek, and F. De Martini, 2005, Phys. Rev. Lett. **95**, 090504.
Ricci, M., F. Sciarrino, C. Sias, and F. De Martini, 2004, Phys. Rev. Lett. **92**, 047901.
Rivest, R. L., A. Shamir, and L. M. Adleman, 1978, Comm. ACM **21**, 120.
Rodriguez-Rosario, C. A., K. Modi, and A. Aspuru-Guzik, 2010, Phys. Rev. A **81**, 012313.
Roubert, B., and D. Braun, 2008, Phys. Rev. A **78**, 042311.
Rybar, T., and M. Ziman, 2008, Phys. Rev. A **78**, 052114.
Saberi, H., and Y. Mardoukhi, 2012, Phys. Rev. A **85**, 052323.
Sabuncu, M., U. L. Andersen, and G. Leuchs, 2007, Phys. Rev. Lett. **98**, 170503.
Sagawa, T., and M. Ueda, 2008, Phys. Rev. A **77**, 012313.
Sanguinetti, B., E. Pomarico, P. Sekatski, H. Zbinden, and N. Gisin, 2010, Phys. Rev. Lett. **105**, 080503.
Scarani, V., and N. Gisin, 2001, Phys. Rev. A **65**, 012311.
Scarani, V., S. Iblisdir, N. Gisin, and A. Acín, 2005, Rev. Mod. Phys. **77**, 1225.
Schon, C., E. Solano, F. Verstraete, J. I. Cirac, and M. M. Wolf, 2005, Phys. Rev. Lett. **95**, 110503.
Sciarrino, F., and F. De Martini, 2005, Phys. Rev. A **72**, 062313.
Sciarrino, F., and F. De Martini, 2007, Phys. Rev. A **76**, 012330.
Sciarrino, F., C. Sias, M. Ricci, and F. De Martini, 2004a, Phys. Lett. A **323**, 34 .
Sciarrino, F., C. Sias, M. Ricci, and F. De Martini, 2004b, Phys. Rev. A **70**, 052305.
Sekatski, P., B. Sanguinetti, E. Pomarico, N. Gisin, and C. Simon, 2010, Phys. Rev. A **82**, 053814.
Shen, Y., L. A. Hao, and G. L. Long, 2011, Chin. Phys. Lett. **28**, 010306.
Shor, P. W., 1994, in *35-th Annual Symposium on Foundations of Computer Science* (IEEE, Los Alamitos, CA), pp. 56–65.
Shor, P. W., and J. Preskill, 2000, Phys. Rev. Lett. **85**, 441.
Simon, C., V. Bužek, and N. Gisin, 2001, Phys. Rev. Lett. **87**, 170405.
Simon, C., G. Weihs, and A. Zeilinger, 2000, Phys. Rev. Lett. **84**, 2993.
Siomau, M., and S. Fritzsche, 2010a, Eur. Phys. J. D **57**, 293.
Siomau, M., and S. Fritzsche, 2010b, Eur. Phys. J. D **60**, 417.
Song, W., and T. Qin, 2008, Commun. Theor. Phys. **49**, 1515.
Soubusta, J., L. Bartuskova, A. Cernoch, M. Dusek, and J. Fiurasek, 2008, Phys. Rev. A **78**, 052323.
Tamaki, K., M. Koashi, and N. Imoto, 2003, Phys. Rev. Lett. **90**, 167904.
Umegaki, U. H., and Ködai, 1962, Math. Sem. Rep. **14**, 59.
Usami, K., Y. Nambu, Y. Tsuda, K. Matsumoto, and K. Nakamura, 2003, Phys. Rev. A **68**, 022314.
Vaidman, L., Y. Aharonov, and D. Z. Albert, 1987, Phys. Rev. Lett. **58**, 14.
Valente, D., Y. Li, J. P. Poizat, L. C. Gérard, L. C. Kwek, M. F. Santos, and A. Auffèves, 2012, Phys. Rev. A **86**, 022333.
Vidal, G., 2003, Phys. Rev. Lett. **91**, 147902.
Vidal, G., J. I. Latorre, P. Pascual, and R. Tarrach, 1999, Phys. Rev. A **60**, 126.

Walgate, J., and L. Hardy, 2002, Phys. Rev. Lett. **89**, 147901.
Walgate, J., A. J. Short, L. Hardy, and V. Vedral, 2000, Phys. Rev. Lett. **85**, 4972.
Walker, T. A., and S. L. Braunstein, 2007, Phys. Rev. Lett. **98**, 080501.
Wang, X. B., T. Hiroshima, A. Tomita, and M. Hayashi, 2007, Phys. Rep. **448**, 1.
Wang, X. W., and G. J. Yang, 2009a, Phys. Rev. A **79**, 062315.
Wang, X. W., and G. J. Yang, 2009b, Phys. Rev. A **79**, 064306.
Wang, X. W., D. Y. Zhang, G. J. Yang, S. Q. Tang, and L. J. Xie, 2011a, Phys. Rev. A **84**, 042310.
Wang, Y. N., H. D. Shi, L. Jing, Z. X. Xiong, J. Lei, L. Z. Mu, and H. Fan, 2012, J. Phys. A-Math. Theor. **45**, 025304.
Wang, Y. N., H. D. Shi, Z. X. Xiong, L. Jing, X. J. Ren, L. Z. Mu, and H. Fan, 2011b, Phys. Rev. A **84**, 034302.
Weedbrook, C., N. B. Grosse, T. Symul, P. K. Lam, and T. C. Ralph, 2008, Phys. Rev. A **77**, 052313.
Weedbrook, C., S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, 2012, Rev. Mod. Phys. **84**, 621.
Wehrl, A., 1978, Rev. Mod. Phys. **50**, 221.
Werner, A. H., T. Franz, and R. F. Werner, 2009, Phys. Rev. Lett. **103**, 220504.
Werner, R. F., 1998, Phys. Rev. A **58**, 1827.
Wootters, W. K., and B. D. Fields, 1989, Ann. Phys.-New York **191**, 363.
Wootters, W. K., and W. H. Zurek, 1982, Nature **299**, 802.
Wootters, W. K., and W. H. Zurek, 2009, Phys. Today **62**, 76.
Wu, F., and X. H. Wu, 2012, Quant. Inf. Process. **11**, 1.
Wu, Y. C., and G. C. Guo, 2011, Phys. Rev. A **83**, 062301.
Xiang, G. Y., T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, 2010, Nat. Photonics **4**, 316.
Xiong, Z. X., H. D. Shi, Y. N. Wang, L. Jing, J. Lei, L. Z. Mu, and H. Fan, 2012, Phys. Rev. A **85**, 012334.
Xu, J. S., C. F. Li, L. Chen, X. B. Zou, and G. C. Guo, 2008, Phys. Rev. A **78**, 032322.
Yan, L. H., Y. F. Gao, and J. G. Zhao, 2009, Int. J. Theor. Phys. **48**, 2445.
Yang, J., Y. F. Yu, Z. M. Zhang, and S. H. Liu, 2008, Phys. Rev. A **77**, 034302.
Yang, S., M. S. Zhao, N. L. Liu, and Z. B. Chen, 2007, Chin. Phys. Lett. **24**, 3048.
Yoshida, M., T. Miyadera, and H. Imai, 2010, Int. Sym. on ISITA , 917.
Yu, L. B., W. H. Zhang, and L. Ye, 2007, Phys. Rev. A **76**, 034303.
Yu, Y. F., J. Feng, X. Q. Zhou, and M. S. Zhan, 2004, Int. J. Theor. Phys. **43**, 21.
Yu, Z. W., 2009, Chin. Phys. Lett. **26**, 080304.
Yuen, H. P., 1986, Phys. Lett. A **113**, 405.
Zanardi, P., 1998, Phys. Rev. A **58**, 3484.
Zavatta, A., J. Fiurasek, and M. Bellini, 2011, Nat. Photonics **5**, 52.
Zhan, X. G., D. Y. Zhang, F. Gao, Y. L. Li, and H. S. Zeng, 2009, Commun. Theor. Phys. **51**, 1023.
Zhan, Y. B., 2005, Phys. Lett. A **336**, 317.
Zhang, C. W., C. F. Li, Z. Y. Wang, and G. C. Guo, 2000a, Phys. Rev. A **62**, 042302.
Zhang, C. W., Z. Y. Wang, C. F. Li, and G. C. Guo, 2000b, Phys. Rev. A **61**, 062310.
Zhang, J., C. D. Xie, and P. van Loock, 2008, Phys. Rev. A **77**, 022316.
Zhang, J., C. D. Xie, and K. C. Peng, 2005, Phys. Rev. Lett. **95**, 170501.
Zhang, J., C. D. Xie, and K. C. Peng, 2006, Phys. Rev. A **73**, 042315.
Zhang, W. H., J. L. Dai, Z. L. Cao, and M. Yang, 2010a, Opt. Commun. **283**, 1956.
Zhang, W. H., J. L. Dai, Z. L. Cao, and M. Yang, 2010b, Opt. Commun. **283**, 3818.
Zhang, W. H., and L. Ye, 2009, Chin. Phys. B **18**, 3702.
Zhang, W. H., L. B. Yu, L. Ye, and J. L. Dai, 2007, Phys. Lett. A **360**, 726.
Zhang, Y. L., Y. N. Wang, X. R. Xiang, L. Jing, L. Z. Mu, V. Korepin, and H. Fan, 2013, Phys. Rev. A (accepted), arXiv:1211.0195 .
Zhang, Z. Y., S. Q. Tang, L. J. Xie, and X. W. Wang, 2012, Int. J. Theor. Phys. **51**, 805.
Zhao, Z., A. N. Zhang, X. Q. Zhou, Y. A. Chen, C. Y. Lu, A. Karlsson, and J. W. Pan, 2005, Phys. Rev. Lett. **95**, 030502.
Zheng, S. B., 2004, Chin. Phys. Lett. **21**, 1689.
Zheng, S. B., 2005, J. Phys. B-Mol. Opt. **38**, 1499.
Zhou, D. L., B. Zeng, and L. You, 2006, Phys. Lett. A **352**, 41.
Zhou, Y. H., 2011, Chin. Phys. B **20**, 080305.
Zhou, Z. W., and G. C. Guo, 2000, Phys. Rev. A **61**, 032108.
Zou, X. B., Y. L. Dong, and G. C. Guo, 2006, Phys. Lett. A **360**, 44.
Zou, X. B., and W. Mathis, 2005, Phys. Rev. A **72**, 022306.
Zou, X. B., K. Pahlke, and W. Mathis, 2003, Phys. Rev. A **67**, 024304.